on networks™
Easy, Reliable & Secure

N300 Wireless ADSL2+ Modemrouter (N300RMB)

Benutzerhandbuch

Dezember 2012
202-11210-01
v1.0

Marken

Marken- und Produktnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber. Informationen können ohne vorherige Ankündigung geändert werden.

Zur Verbesserung des internen Designs, des Betriebs und/oder der Zuverlässigkeit behält On Networks sich das Recht vor, die in diesem Dokument beschriebenen Produkte ohne vorherige Ankündigung zu ändern. On Networks lehnt im Zusammenhang mit dem Einsatz oder der Anwendung der hier beschriebenen Produkte oder Schaltpläne jegliche Haftung ab.

Inhalt

Kapitel 1 Hardware-Konfiguration

Lieferumfang Ihres Modemrouters 8
Positionieren des Modemrouters 8
Hardware-Funktionen 9
Vorderseite 9
Rückseite 11
Reset-Knopf an der Seite 11
Symbol 12
ADSL-Mikrofilter 12
Einfacher ADSL-Mikrofilter 13
ADSL-Mikrofilter mit integriertem Splitter 13
Anschließen des Modemrouters 14
Tipps zur Herstellung von Verbindungen zum Modemrouter 17

Kapitel 2 Erste Schritte

Vorbereitung der Modemrouterkonfiguration 19
Verwenden der Standard-TCP/IP-Eigenschaften für DHCP 19
Sammeln von ISP-Informationen 19
Wireless-Geräte und Sicherheitseinstellungen 19
Anmelde- und Zugriffsarten 19
Anmelden am Modemrouter 20
Anmeldung nicht erfolgreich 21
Manuelle Abmeldung 21
Aktualisieren der Firmware 21
Startbildschirm (Dashboard) 22
EZ Setup-Assistent 23
Herstellen einer Verbindung mit einem WLAN-Netzwerk 24
WPS-Methode 24
Manuelle Methode 25

Kapitel 3 Modemrouter Konfiguration

Internetkonfiguration (Grundeinstellungen) 27
ADSL-Einstellungen 30
Voreingestellte Sicherheit 30
Grundlagen der WLAN-Sicherheit 31
SSID-Broadcast deaktivieren 31
Einschränkung des Zugriffs über MAC-Adressen 32
WLAN-Sicherheitsoptionen 32

WLAN-Konfiguration 32
Überprüfen jedes Geräts in Ihrem Netzwerk 33
Wireless-Konfiguration anzeigen und bearbeiten 33
Felder auf dem Bildschirm Wireless Settings (Wireless-Konfiguration) 34
Ändern der WPA-Sicherheitsoption und Passphrase 35
Gastnetzwerk 35
WAN-Konfiguration 36
DMZ-Standardserver 37
Ändern der MTU-Größe 37
LAN Setup (LAN Konfigurieren) 39
Verwenden des Modemrouters als DHCP-Server 41
Adressreservierung 42
QoS (Quality of Service)-Konfiguration 43

Kapitel 4 Sicherheitseinstellungen

Regeln für die Firewall zur Steuerung des Netzwerkzugangs 49
Eingangsregeln (Portweiterleitung) 49
Ausgangsregeln (Dienstsperren) 49
Webseiten sperren 50
Regeln für die Firewall zur Steuerung des Netzwerkzugangs 51
Regeln für die Firewall konfigurieren 51
Zeitzone einstellen 52
Zeitplan für Dienstsperren 53
Konfigurieren von E-Mail-Warnmeldungen 54
Portweiterleitung und Port-Triggering 55
Grundlegende Informationen zum Remote-Computerzugriff 56
Port-Triggering zum Öffnen eingehender Ports 57
Portweiterleitung zur Zulassung externer Hostkommunikation 58
Unterschiede zwischen Portweiterleitung und Port-Triggering 59
Konfigurieren der Portweiterleitung an lokale Server 60
Hinzufügen eines benutzerdefinierten Diensts 61
Portweiterleitungseintrag bearbeiten oder löschen 61
Anwendungsbeispiel: Veröffentlichen eines lokalen Webservers 62
Konfigurieren des Port-Triggering 62

Kapitel 5 Netzwerkverwaltung

Modemrouter-Firmware aktualisieren 66
Automatische Firmwareprüfung 66
Nach Firmware-Upgrades suchen 67
Sichern der Einstellungen 67
Sichern 68
Wiederherstellen 68
Löschen 68
Passwort ändern 68
Passwortwiederherstellung 69

Routerstatus anzeigen 70
Router-Informationen 70
Internet-Porteinstellungen. 71
WLAN-Einstellungen und Gastnetzwerke (2,4GHz). 73
Angeschlossene Geräte anzeigen 73
Protokolle 74

Kapitel 6 Erweiterte Einstellungen

Erweiterte WLAN-Konfiguration 76
Einschränkung des WLAN-Zugriffs über MAC-Adressen. 77
WLAN-Repeating (WDS) 78
WLAN-Repeating 80
Konfigurieren der Basisstation 81
Konfigurieren eines Repeaters. 82
Dynamisches DNS 82
Statische Routen 83
Fernsteuerung 85
Universal Plug and Play 86
Ändern des Gerätemodus 88

Kapitel 7 Virtual Private Networking

Erstellen einer Gateway-zu-Gateway VPN-Konfiguration 90
VPN-Assistent 91
Aktivieren eines VPN-Tunnels 93
Prüfen des Status eines VPN-Tunnels. 94
Deaktivieren eines VPN-Tunnels 95
Konfiguration von VPN-Tunneln mithilfe der automatischen Regel 96
Konfiguration von VPN-Tunneln mithilfe der manuellen Regel 100

Kapitel 8 Fehlerbehebung

Beheben von Fehlern im Zusammenhang mit LEDs 104
Power-LED leuchtet nicht. 104
Power-LED leuchtet rot. 105
Netzwerk-LED leuchtet nicht 105
Anmeldung am Modemrouter nicht möglich. 105
Beheben von Fehlern bei der Internetverbindung 106
ADSL-Verbindung. 106
Internet-LED leuchtet rot. 107
Abrufen einer Internet IP-Adresse 107
Beheben von Fehlern im Zusammenhang mit PPPoE oder PPPoA 108
Fehlerbehebung im Zusammenhang mit dem Internetzugriff. 109
TCP/IP-Netzwerk reagiert nicht 109
Testen des LAN-Pfads zum Modemrouter 109
Testen des Pfads vom Computer zu einem Remote-Gerät 110

Änderungen werden nicht gespeichert 111
Falsches Datum oder falsche Uhrzeit 111

Anhang A Zusatzinformationen

Werkseinstellungen 113
Technische Daten 115

Anhang B Konformitätserklärung

Hardware-Konfiguration

1

Ihr Modemrouter

Sie können mit dem N300 Wireless ADSL2+ Modemrouter (N300RMB) einfach und sicher ein drahtloses Heimnetzwerk mit schnellem Zugriff auf das Internet über eine Hochgeschwindigkeits-DSL-Verbindung einrichten. DerModemrouter besitzt ein integriertes DSL-Modem und ist kompatibel zu allen größeren DSL-Internetanbietern. Mit dem Modemrouter können Sie unsichere Inhalte und Anwendungen aus dem Internet sperren. Außerdem schützt er Ihre Geräte (Computer, Spielekonsolen usw.), mit denen Sie eine Verbindung zu Ihrem Heimnetzwerk herstellen.

In diesem Kapitel wird die Konfiguration der Hardware erläutert. Wenn Sie den Modemrouter bereits konfiguriert haben, können Sie dieses Kapitel überspringen. In Kapitel 2 wird die Konfiguration der Internetverbindung erläutert.

Dieses Kapitel enthält die folgenden Abschnitte:

- *Lieferumfang Ihres Modemrouters*
- *Positionieren des Modemrouters*
- *Hardware-Funktionen*
- *ADSL-Mikrofilter*
- *Anschließen des Modemrouters*

Lieferumfang Ihres Modemrouters

Öffnen Sie den Karton, und nehmen Sie den Modemrouter, die Kabel und die Installationsanleitung heraus.

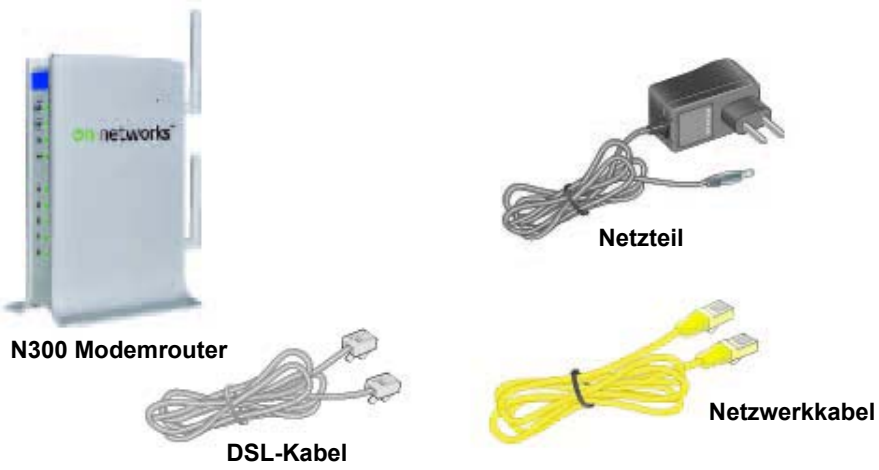


Abbildung 1. Überprüfen des Packungsinhalts

Falls einer dieser Teile fehlt, beschädigt ist oder zu einem anderen Modell gehört, wenden Sie sich bitte an Ihren On Networks-Fachhändler. Bewahren Sie den Karton sowie das Original-Verpackungsmaterial für den Fall auf, dass Sie das Produkt zu einem späteren Zeitpunkt zur Reparatur einsenden müssen.

Positionieren des Modemrouters

Der Modemrouter ermöglicht Ihnen den Zugriff auf Ihr Netzwerk von jedem Standort innerhalb des WLAN-Radius. Durch die richtige Aufstellung Ihres Modemrouter können Sie jedoch maßgeblich dazu beitragen, die Reichweite Ihres WLAN zu erhöhen. Zum Beispiel kann die Reichweite des Signals durch die Stärke und Anzahl der Wände, die das Signal durchdringt, eingeschränkt werden. Beste Ergebnisse erzielen Sie bei der Wahl folgender Standorte für Ihren Modemrouter:

- Möglichst nahe am Zentrum des Bereichs, in dem sich Ihre Computer und anderen Geräte befinden, und vorzugsweise in Sichtverbindung zu allen Wireless-Geräten
- In der Nähe einer Steckdose und in Reichweite der Netzwerkkabel Ihrer kabelgebundenen Computer
- In erhöhter Position wie beispielsweise auf einem Wandregal, wobei sich zwischen dem Modemrouter und den anderen Geräten möglichst wenige Wände und Decken befinden sollten
- Nicht in der Nähe von elektronischen Geräten, die Störungen verursachen können Zu Geräten, die Störungen verursachen können, zählen Deckenventilatoren, Alarmanlagen, Mikrowellengeräte, Computer, Basisstationen von schnurlosen Telefonen oder schnurlose 2,4-GHz-Telefone.

- Nicht in der Nähe größerer Metalloberflächen wie massiven Metalltüren oder Aluminiumteilen. Größere Flächen aus Materialien wie Glas, Ziegelstein oder Beton sowie Dämmplatten, Aquarien oder Spiegel können das Signal ebenfalls beeinträchtigen.

Bei Verwendung mehrerer Access Points empfiehlt es sich, nicht die Funkfrequenzkanäle zu wählen, die bereits von den benachbarten Access Points verwendet werden, um Störungen zu reduzieren. Der empfohlene Abstand der Kanäle benachbarter Access Points beträgt 5 Kanäle (verwenden Sie beispielsweise die Kanäle 1 und 6 oder 6 und 11).

Hardware-Funktionen

Nehmen Sie sich einen Moment Zeit, um sich mit dem Etikett, der Vorder- und Rückseite und den Seiten vertraut zu machen, bevor Sie den Modemrouter anschließen. Achten Sie dabei besonders auf die LEDs auf der Vorderseite.

Vorderseite

Auf der Vorderseite des Modemrouters befinden sich zwei Tasten und Status-LEDs.

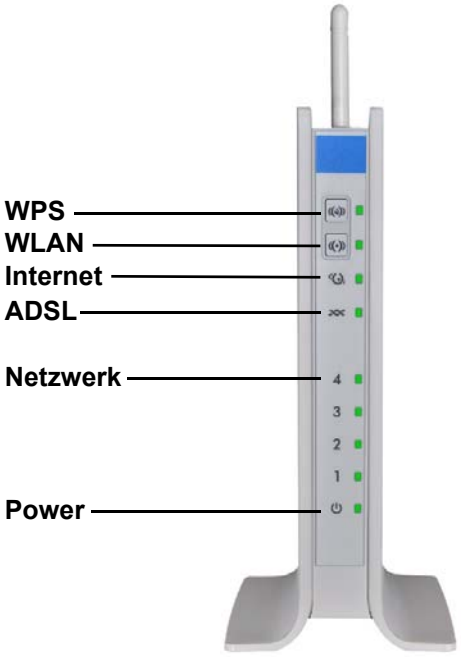


Abbildung 2. Vorderseite des Modemrouters

Tabelle 1. Tasten- und LED-Beschreibungen

Symbol	Beschreibung
WPS	Mit WPS (Wi-Fi Protected Setup) können Sie eine Verbindung zu einem sicheren WLAN-Netzwerk herstellen, ohne das Passwort einzugeben. Siehe *WPS-Methode* auf Seite 24. • **Leuchtet grün**. Ein WPS-fähiges Gerät ist mit dem Router verbunden. • **Blinkt grün**. WPS-Verbindung mit WPS-fähigem Gerät wird aufgebaut. • **Aus**. Keine WPS-Verbindung.
WLAN	Sie können auf die WLAN-Taste drücken, um das WLAN zu aktivieren bzw. zu deaktivieren. • **Blinkt grün**. Daten werden über die drahtlose Verbindung übertragen oder empfangen. • **Aus**. Die WLAN-Funktion ist deaktiviert.
Internet	• **Leuchtet grün**. Es besteht eine Internetverbindung. • **Blinkt grün**. Es werden Daten über den Internetanschluss übertragen. • **Stetig rot**. Es konnte keine Verbindung zum Internet hergestellt werden. • **Aus**. Keine Internetverbindung.
ADSL	• **Leuchtet grün**. Sie verfügen über eine DSL-Verbindung. Technisch gesehen ist der DSL-Port mit der Gegenstelle Ihres ISP synchronisiert. • **Blinkt grün**. Der Modemrouter handelt gerade die bestmögliche Geschwindigkeit der DSL-Verbindung aus. • **Aus**. Das Gerät ist abgeschaltet, es besteht keine DSL-Verbindung.
Netzwerk (1-4)	• **Leuchtet grün**. Am LAN-Port wurde eine Netzwerkverbindung mit einem Gerät erkannt, z. B. einem Computer. • **Blinkt grün**. Daten werden übertragen oder empfangen. • **Aus**. An diesem Port wurde keine Verbindung erkannt.
Power/ Test	• **Leuchtet grün**. Der Modemrouter wird mit Strom versorgt. • **Blinkt grün**. Der Router startet. • **Stetig rot**. Fehler beim Selbsttest (Power-On Self-Test, POST), oder es ist eine Fehlfunktion des Geräts aufgetreten. • **Aus**. Der Modemrouter wird nicht mit Strom versorgt.

Rückseite

An der Rückseite befinden sich die in der folgenden Abbildung dargestellten Verbindungen.

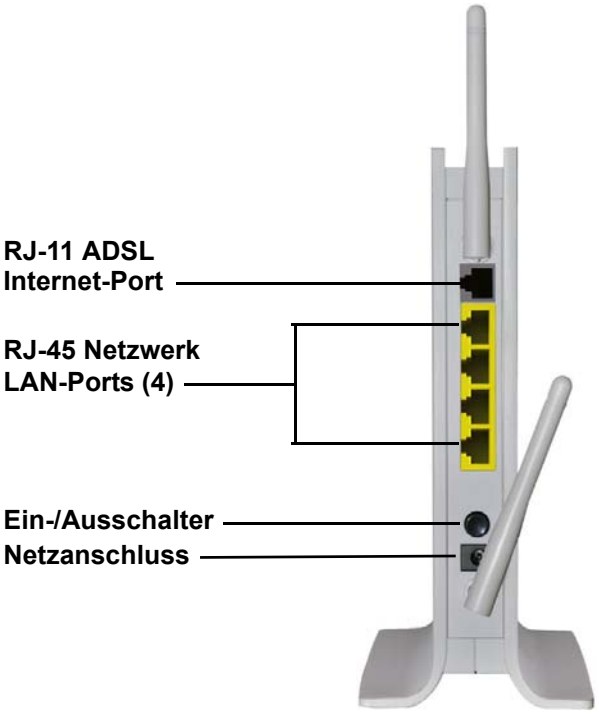
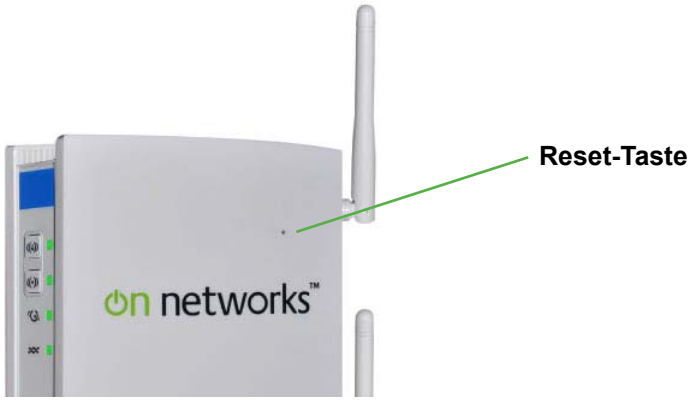


Abbildung 3. Rückseite des Routers

Weitere Informationen zum Zurücksetzen der Werkseinstellungen finden Sie unter *Werkseinstellungen* auf Seite 113.

Reset-Knopf an der Seite

Verwenden Sie die Reset-Taste, um den Modemrouter auf die Werkseinstellungen zurückzusetzen.



- **Zurücksetzen des Modemrouters:**

  Verwenden Sie zum Zurücksetzen des Routers einen spitzen Gegenstand (z. B. eine Büroklammer), und halten Sie damit die **Reset**-Taste mindestens 7 Sekunden lang gedrückt.

Informationen zu den Werkseinstellungen finden Sie unter*Werkseinstellungen* auf Seite 113.

Symbol

Das Etikett auf der Unterseite des Modemrouters enthält den voreingestellten WLAN-Netzwerknamen und das Passwort, Anmeldeinformationen, die MAC-Adresse und die Seriennummer.

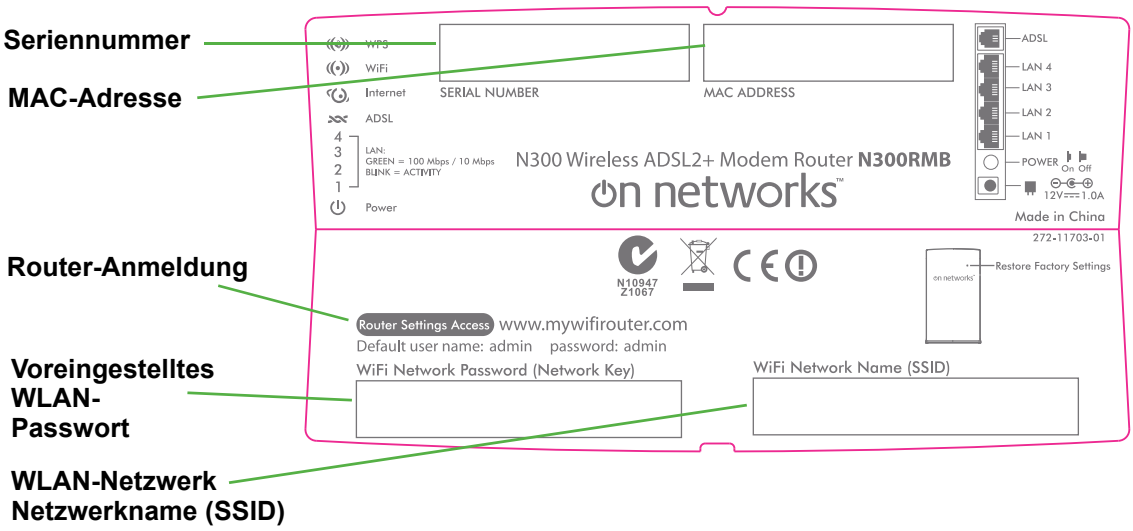


Abbildung 4. Auf dem Etikett werden eindeutige Informationen zu Ihrem Modem angegeben

ADSL-Mikrofilter

Wenn Sie zum ersten Mal eine Kabelverbindung zwischen einer DSL-Telefonleitung und Ihrem Computer oder Laptop mittels Modem hergestellt haben, sind Sie eventuell noch nicht mit ADSL-Mikrofiltern vertraut. Falls doch, so können Sie diesen Abschnitt überspringen und mit *Anschließen des Modemrouters* auf Seite 14 fortfahren.

Ein ADSL-Mikrofilter ist ein kleines In-Line-Gerät, das DSL-Interferenzen aus den Standardtelefonendgeräten herausfiltert, die die gleiche Leitung wie Ihr DSL-Anschluss verwenden. Jedes Telefonendgerät, das mit einem Festnetzanschluss verbunden ist, der auch einen DSL-Anschluss beinhaltet, benötigt einen ADSL-Mikrofilter zum Herausfiltern der DSL-Interferenz. Zu den Geräten gehören Telefone, Faxgeräte, Anrufbeantworter und Displays, auf denen die Nummer des Anrufers angezeigt wird. Nicht jede Festnetzleitung bei Ihnen zu Hause enthält auch automatisch einen DSL-Anschluss. Ob ein DSL-Anschluss benötigt wird, hängt von der Konfiguration des DSL-Anschlusses bei Ihnen zu Hause ab.

Hinweis: Oftmals befindet sich der ADSL-Mikrofilter in der Box mit dem Modemrouter. Sollten Sie den Modemrouter in einem Land gekauft haben, für das kein Mikrofilter im Lieferumfang enthalten ist, erhalten Sie diesen in der Regel von Ihrem Internet-Anbieter.

Einfacher ADSL-Mikrofilter

➢ **So verwenden Sie einen einfachen ADSL-Mikrofilter:**

1. Stecken Sie das Kabel des ADSL-Mikrofilters in die Wandbuchse.
2. Stecken Sie das Kabel Ihres Telefonendgeräts in die Telefonbuchse.

   Der Modemrouter wird direkt mit einer separaten DSL-Leitung verbunden. Schließt man den WLAN-Modemrouter an die Telefonbuchse an, so wird dadurch die Internetverbindung blockiert.

Abbildung 5. Einfacher ADSL-Mikrofilter

Falls Sie über keine separate DSL-Leitung für den Modem verfügen, verwenden Sie am besten einen ADSL-Mikrofilter mit einem integrierten Splitter. Siehe *ADSL-Mikrofilter mit integriertem Splitter* auf Seite 13. Sie können auch separat einen Splitter erwerben.

➢ **So verwenden Sie einen separaten Splitter:**

1. Schließen Sie den Splitter an die Telefonbuchse an.
2. Verbinden Sie den Telefonfilter mit dem Splitter.
3. Schließen Sie das Telefon an den Telefonfilter an.
4. Verbinden Sie den Modem mit einer der anderen Buchsen des separaten Splitters.

ADSL-Mikrofilter mit integriertem Splitter

Verwenden Sie einen ADSL-Mikrofilter mit integriertem Splitter, wenn es nur einen einzigen Anschluss an der Telefondose gibt, über den Sie sowohl zum Modemrouter als auch zum Telefon eine Verbindung herstellen möchten.

➢ **So verwenden Sie einen ADSL-Filter/Splitter (Zwei Leitungen):**

1. Stecken Sie das Kabel des ADSL-Mikrofilters in die DSL-Wandbuchse.
2. Stecken Sie das Kabel Ihres Telefonendgeräts in die Telefonbuchse.

3. Verbinden Sie das WLAN-Modem Modem mit der ADSL-Buchse.

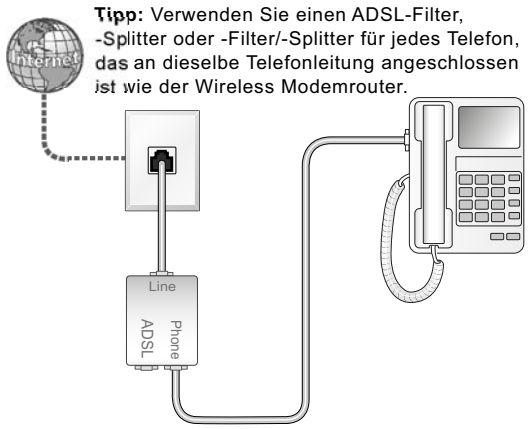
Abbildung 6. ADSL-Mikrofilter mit integriertem Splitter

Anschließen des Modemrouters

Auf der mitgelieferten Installationsanleitung finden Sie ein Verkabelungsdiagramm. In diesem Abschnitt wird mit detaillierten Illustrationen beschrieben, wie Sie Ihren Modem anschließen können.

➢ **So schließen Sie Ihren Modem an:**

1. Installieren Sie, wie hier dargestellt, einen ADSL-Mikrofilter zwischen Telefonleitung und Telefon. Die Abbildung zeigt eine Kombination aus Mikrofilter/Splitter für zwei Leitungen. Stecken Sie, wie hier dargestellt. das Kabel Ihres Telefonendgeräts in die Telefonbuchse.

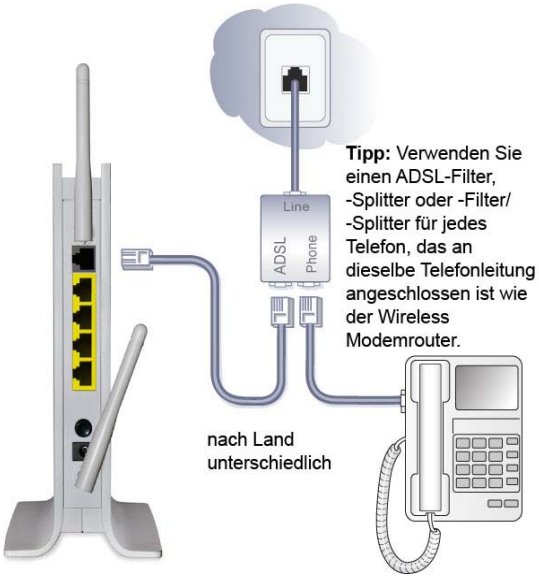

Tipp: Verwenden Sie einen ADSL-Filter, -Splitter oder -Filter/-Splitter für jedes Telefon, das an dieselbe Telefonleitung angeschlossen ist wie der Wireless Modemrouter.
Internet
Line
ADSL
Phone

2. Verwenden Sie das mitgelieferte ADSL-Anschlusskabel mit dem ADSL-Port (A) desModemrouters mit dem ADSL-Port (B) der Filter/Splitter-Kombination.

VORSICHT:

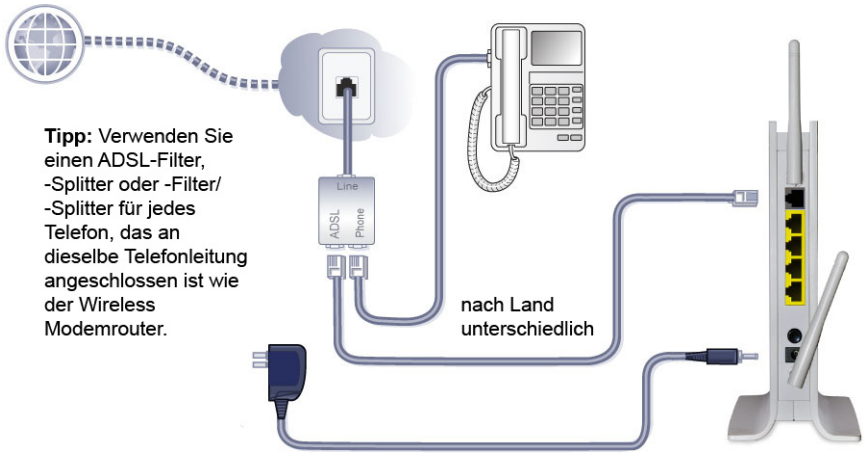
Falsches Anschließen eines Filters an Ihren Modemrouter blockiert Ihre DSL-Verbindung.

3. Schließen Sie den ADSL-Port des Modemrouters an den ADSL-Port des Filters/Splitters an.


Tipp: Verwenden Sie einen ADSL-Filter, -Splitter oder -Filter/ -Splitter für jedes Telefon, das an dieselbe Telefonleitung angeschlossen ist wie der Wireless Modemrouter.
Line
ADSL
Phone
nach Land unterschiedlich

Wenn Ihr Modemrouter und Ihr Telefon an dieselbe Telefonleitung angeschlossen sind, verwenden Sie für jedes Telefon im Haus einen ADSL-Filter/Splitter.

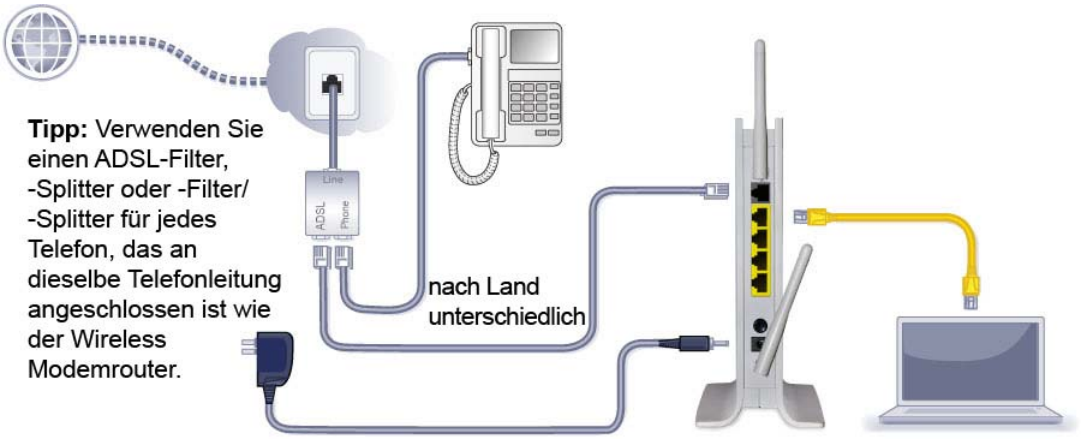
4. Schalten Sie den Modemrouter ein.


Tipp: Verwenden Sie einen ADSL-Filter, -Splitter oder -Filter/ -Splitter für jedes Telefon, das an dieselbe Telefonleitung angeschlossen ist wie der Wireless Modemrouter.
Line
ADSL
Phone
nach Land unterschiedlich

   a. Schließen Sie das Netzteil an den Router an, und stecken Sie es in eine Steckdose.
   b. Warten Sie, bis die WLAN-LED an der Vorderseite leuchtet. Leuchtet keine der LEDs an der Vorderseite, drücken Sie die Taste **Power On/Off** (Ein-/Aus) an der Rückseite des Modemrouters.

5. Schließen Sie einen Computer an.

   Sie können hierzu ein Netzwerkkabel verwenden oder eine kabellose Verbindung herstellen.


Tipp: Verwenden Sie einen ADSL-Filter, -Splitter oder -Filter/ -Splitter für jedes Telefon, das an dieselbe Telefonleitung angeschlossen ist wie der Wireless Modemrouter.
Line
ADSL
Phone
nach Land unterschiedlich

- Verwenden Sie das gelbe Netzwerkkabel, um Ihren Computer mit einem Netzwerkanschluss am Modem zu verbinden.
- Stellen Sie optional eine kabellose Verbindung her, indem Sie die voreingestellten WLAN-Sicherheitseinstellungen verwenden, die auf dem Etikett an der Unterseite des Routers angegeben sind.

6. Öffnen Sie einen Browser.

   Wenn das erste Mal eine Verbindung zum Modem aufgebaut wird, öffnet der Browser automatisch einen ModemrouterBildschirm, der Ihnen dabei hilft, Ihre Internetverbindung einzurichten.

on networks™
N300RM
Konfigurieren der Internetverbindung
Sie sind noch nicht mit dem Internet verbunden.
Benötigen Sie Hilfe von On Networks ?
Ja
Nein, ich möchte die Internetverbindung selbst konfigurieren.
Ich habe die Routereinstellungen gespeichert und möchte den Router auf diese Einstellungen zurücksetzen.
Weiter

   Erscheint diese Anzeige nicht, sehen Sie bitte unter dem Abschnitt *Tipps zur Herstellung von Verbindungen zum Modemrouter* auf Seite 17 nach.

   Wenn Sie bereits mit dem Modem verbunden sind und dieser Bildschirm angezeigt wurde, werden Sie dazu aufgefordert, sich anzumelden. Siehe *Anmelden am Modemrouter* auf Seite 20.

7. Schließen Sie weitere Computer an Ihren Modemrouter an, indem Sie jeweils ein Netzwerkkabel eines PCs in einen der drei übrigen LAN-Ports stecken.

   Hinweis: *Um mehrere Modemrouter mit demselben Netzwerk verbinden zu können, müssen Sie den Gerätemodus in den Modem-Modus setzen. Siehe Ändern des Gerätemodus auf Seite 88.*

Tipps zur Herstellung von Verbindungen zum Modemrouter

Wenn der Browser die Website nicht anzeigt, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass der Computer an einen der vier Netzwerk-LAN-Ports angeschlossen oder per WLAN mit dem Modemrouter verbunden ist.
- Stellen Sie sicher, dass der Modem komplett eingeschaltet ist und die WLAN-LED leuchtet.
- Schließen und öffnen Sie den Browser erneut, um sicherzustellen, dass der Browser nicht die vorherige Seite zwischenspeichert.
- Rufen Sie die Adresse **http://www.mywifirouter.com** (oder **http://192.168.0.1/index.htm**) auf.
- Wenn dem Computer eine statische oder feste IP-Adresse zugeordnet ist (das ist ungewöhnlich), ändern Sie diese Einstellung, damit der PC automatisch eine IP-Adresse vom Modemrouter bezieht.

Wenn derModemrouter keine Verbindung mit dem Internet herstellt, gehen Sie wie folgt vor:

1. Überprüfen Sie sämtliche Einstellungen, um sicherzustellen, dass Sie die richtigen Optionen gewählt und alles korrekt eingegeben haben.
2. Wenden Sie sich an Ihren Provider und vergewissern Sie sich, dass Ihnen die richtigen Konfigurationsdaten vorliegen.

2 Erste Schritte

Anmeldung am Router Modem

In diesem Kapitel wird die Anmeldung und Einrichtung Ihres Modemrouters nach dem Anschließen der Hardware gemäß den Anweisungen in der Installationsanleitung und im vorhergehenden Kapitel behandelt.

Dieses Kapitel enthält die folgenden Abschnitte:

- *Vorbereitung der Modemrouterkonfiguration*
- *Anmelde- und Zugriffsarten*
- *Anmelden am Modemrouter*
- *Aktualisieren der Firmware*
- *Startbildschirm (Dashboard)*
- *EZ Setup-Assistent*
- *Herstellen einer Verbindung mit einem WLAN-Netzwerk*

Vorbereitung der Modemrouterkonfiguration

Bevor Sie mit der Konfiguration beginnen, müssen Sie jedoch Ihre ISP-Informationen zur Hand haben und sicherstellen, dass die Computer und anderen Geräte im Netzwerk mit den hier beschriebenen Einstellungen eingerichtet sind.

Verwenden der Standard-TCP/IP-Eigenschaften für DHCP

Wenn Sie den Computer für die Verwendung einer statischen IP-Adresse konfiguriert haben, müssen Sie die Einstellungen ändern, damit DHCP (Dynamic Host Configuration Protocol) verwendet wird.

Sammeln von ISP-Informationen

Wenn Sie einen DSL-Breitbandanschluss haben, benötigen Sie möglicherweise die folgenden Informationen, um Ihren Modemrouter zu konfigurieren und zu überprüfen, ob das Internet richtig konfiguriert ist. Normalerweise müssten Sie alle Informationen, die Sie zur Verbindung mit dem Internet benötigen, von Ihrem Internet-Provider (ISP) erhalten haben. Wenn Sie diese Informationen nicht finden können, bitten Sie Ihren ISP darum, diese bereitzustellen. Wenn die Internetverbindung steht, benötigen Sie das Anmeldeprogramm des ISP auf Ihrem Computer nicht mehr für den Internetzugriff. Beim Start einer Internetanwendung meldet der Modemrouter Sie automatisch an. Stellen Sie sicher, dass Ihnen folgende Informationen vorliegen:

- Die Konfigurationsdaten vom ISP für Ihr DSL-Konto
- Benutzername und Passwort vom ISP zur Anmeldung
- Einstellungen für eine feste oder statische IP-Adresse (besondere Bereitstellung vom ISP; dies kommt selten vor.)

Wireless-Geräte und Sicherheitseinstellungen

Stellen Sie sicher, dass das von Ihnen verwendete Wireless-Gerät bzw. der verwendete Computer die WPA- oder WPA2-WLAN-Sicherheit unterstützt. Dies sind die vom Modemrouter unterstützten WLAN-Sicherheitseinstellungen.

Anmelde- und Zugriffsarten

Es gibt verschiedene Anmeldearten mit unterschiedlichem Zweck. Es ist wichtig, dass Sie den Unterschied verstehen, damit Sie wissen, wann Sie welche Anmeldung verwenden müssen.

- Bei der **Modemrouter-Anmeldung** werden Sie bei der Benutzeroberfläche des Modemrouters angemeldet.

- Bei der **ISP-Anmeldung** werden Sie beim Internet-Provider angemeldet. Ihr Provider hat Ihnen diese Anmeldedaten in einem Brief oder auf andere Weise zukommen lassen. Wenn Ihnen diese Anmeldeinformationen nicht vorliegen, wenden Sie sich bitte an Ihren Provider.
- **WLAN-Schlüssel oder Passwort**: Der Modemrouter verfügt über eine Voreinstellung mit einem eindeutigen Netzwerknamen (SSID) und einem Passwort für den WLAN-Zugriff. Diese Informationen befinden sich auf einem Etikett an der Unterseite des Modemrouters.

Anmelden am Modemrouter

Beim ersten Verbinden mit dem Modemrouter erscheint der Installationsbildschirm. Nach der Erstkonfiguration können Sie sich am Modemrouter anmelden, um die Einstellungen anzuzeigen oder zu ändern.

➢ **So melden Sie sich an:**

1. Geben Sie in den Internetbrowser die Adresse **http://www.mywifirouter.com** (oder **http://192.168.0.1/index.htm**) ein.

2. Geben Sie **admin** als Benutzernamen und **admin** als Passwort ein. Beide Wörter müssen klein geschrieben werden.

Hinweis: Wie bereits im vorherigen Abschnitt erwähnt, unterscheiden sich der Benutzername und das Passwort des Modemrouters von dem Benutzernamen und dem Passwort für die Anmeldung zum Herstellen einer Internetverbindung.

Wenn Sie bei der Anmeldung mit dem Internet verbunden sind, wird der Bildschirm **Firmware Upgrade Assistant** (Assistent für die Aktualisierung der Firmware) angezeigt, sodass Sie eine Aktualisierung der Firmware durchführen können.

Es wird eine Meldung angezeigt, die Sie darüber informiert, ob der Router eine neuere Firmware-Version erkannt hat.

3. Klicken Sie zur Aktualisierung auf die neue Firmware auf **Yes** (Ja), um zuzulassen, dass der Router die neue Firmware-Datei von On Networks herunterlädt und installiert.

WARNUNG:

Achten Sie beim Hochladen der Firmware auf den Modemrouter darauf, dass der Vorgang *nicht* unterbrochen wird (z. B. durch Schließen des Browserfensters, Klicken auf einen Link oder Laden einer neuen Seite). Wenn eine Unterbrechung im Browser stattfindet, wird die Firmware möglicherweise fehlerhaft installiert.

Nach dem Hochladen der Firmware wird der Modemrouter neu gestartet. Der Aktualisierungsvorgang dauert in der Regel ungefähr eine Minute.

Anmeldung nicht erfolgreich

➢ **Gehen Sie folgendermaßen vor, wenn die Anmeldeaufforderung nicht angezeigt wird:**

1. Prüfen Sie die LEDs auf der Vorderseite des Modemrouters, um sicherzustellen, dass der Modemrouter richtig angeschlossen wurde, eingeschaltet ist und das Netzwerkkabel zwischen dem Computer und dem Modemrouter an einen LAN-Port angeschlossen ist.
2. Wenn Sie das Netzwerkkabel angeschlossen und kurz darauf mit dem Browser die URL des Modemrouters aufgerufen haben, benötigt Ihr Computer eventuell eine Weile zur Erkennung der LAN-Verbindung. Starten Sie Ihren Browser neu, und versuchen Sie es erneut.
3. Falls beim WLAN-Zugriff auf den Modemrouter Probleme auftreten, empfiehlt On Networks, während der Konfiguration ein Netzwerkkabel für die Verbindung mit dem Computer zu verwenden, damit Sie sich am Modemrouter anmelden können.
4. Falls Sie keine Verbindung zum Modemrouter herstellen können, überprüfen Sie die Eigenschaften des Internetprotokolls (TCP/IP) der Netzwerkverbindung in der Systemsteuerung Ihres Windows Computers. Stellen Sie dort sicher, dass Ihr Computer IP-Adresse und DNS-Server-Adresse automatisch bezieht. Weitere Informationen finden Sie in der Dokumentation Ihres Computers.

Manuelle Abmeldung

Die Modemrouter-Benutzeroberfläche stellt einen Abmeldebefehl bereit. Dieser befindet sich im unteren Bereich des Modemrouter-Menüs. Melden Sie sich ab, wenn Sie den Computer voraussichtlich für längere Zeit verlassen.

Aktualisieren der Firmware

Wenn Sie bei der Anmeldung mit dem Internet verbunden sind, wird der Bildschirm **Firmware Upgrade Assistant** (Assistent für die Aktualisierung der Firmware) angezeigt, sodass Sie eine Aktualisierung der Firmware durchführen können.

➢ **So aktualisieren Sie die Firmware:**

1. Klicken Sie auf **Yes** (Ja), um nach neuer Firmware zu suchen (empfohlen). Der Modemrouter sucht nach neuer Firmware.
2. Falls keine neue Firmware verfügbar ist, klicken Sie zum Beenden auf **No** (Nein). Sie können später nach neuer Firmware suchen.
3. Falls neue Firmware verfügbar ist, klicken Sie auf **Yes** (Ja), um den Router mit der neuesten Firmware zu aktualisieren. Nach der Aktualisierung wird der Modemrouter neu gestartet.

VORSICHT:

Stellen Sie keine Internetverbindung her, schalten Sie den Modemrouter nicht aus, fahren Sie den Computer nicht herunter, und führen Sie keine anderen Vorgänge aus, bis der Modemrouter neu gestartet wurde und die Power-LED nicht mehr blinkt.

Sie können keine Aktualisierung der Firmware durchführen, solange Sie nicht Ihre Internetverbindung wie unter *EZ Setup-Assistent* auf Seite 23 beschrieben eingerichtet haben.

Startbildschirm (Dashboard)

Mithilfe der Modemrouter-Benutzeroberfläche können Sie die Einstellungen des Modemrouters anzeigen und ändern. In der linken Spalte befinden sich die Menüs. Die derzeit ausgewählte Menüoption ist der Hauptbildschirm.

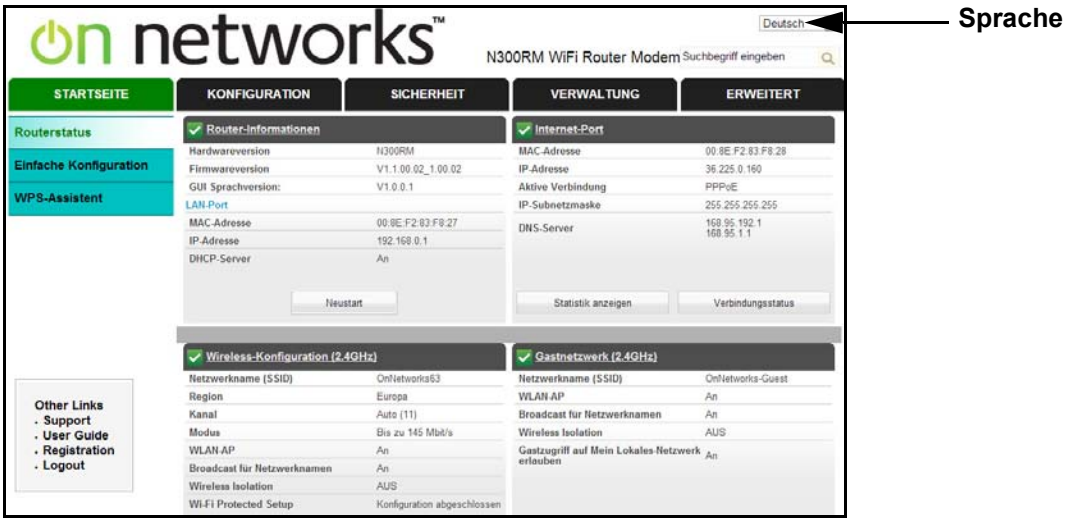


Abbildung 7. Dashboard (Startbildschirm)

- **EZ Setup-Assistent:** Geben Sie die Sprache und den Ort an; automatische Erkennung der Internetverbindung. Siehe *EZ Setup-Assistent* auf Seite 23.

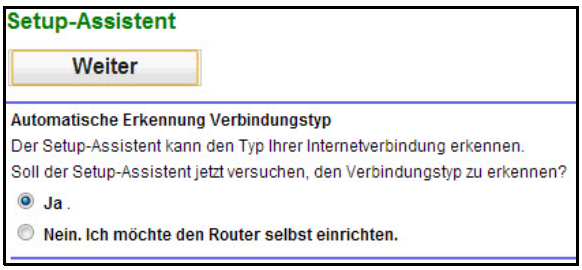
- **WPS Setup** (WPS-Konfiguration): Herstellen einer Verbindung mit dem sicheren WLAN-Netzwerk ohne Eingabe des Passworts. Siehe *Herstellen einer Verbindung mit einem WLAN-Netzwerk* auf Seite 24.
- Registerkarte **Setup** (Konfiguration): Konfiguration, Aktualisierung und Überprüfung des ISP sowie der WLAN-Einstellungen Ihres Modemrouters. Siehe *Kapitel 3, Modemrouter Konfiguration*.
- Registerkarte **Security** (Sicherheit): Anzeige und Konfiguration der Firewall-Einstellungen Ihres Modemrouters, damit keine fragwürdigen Inhalte auf Ihre Computer gelangen. Siehe *Kapitel 4, Sicherheitseinstellungen*.
- Registerkarte **Management** (Verwaltung): Administration des Modemrouters und Netzwerks. Siehe *Kapitel 5, Netzwerkverwaltung*.
- Registerkarte **Advanced** (Erweitert): Konfigurieren des Modemrouters für einmalige Situationen, etwa wenn Remote-Zugriff über IP oder Domainname über das Internet benötigt wird. Für die Verwendung dieses Menüs sind solide Netzwerkkenntnisse erforderlich. Siehe *Kapitel 6, Erweiterte Einstellungen*.
- **Other Links** (Andere Links): Auf der Supportwebsite erhalten Sie Informationen, Hilfe und Produktdokumentationen. Sie können diese Links verwenden, wenn Sie eine Verbindung mit dem Internet hergestellt haben.

EZ Setup-Assistent

Sie können sich am Modemrouter anmelden und mit **EZ Setup** (Einfache Konfiguration) Ihre Internetverbindung konfigurieren.

➢ **So verwenden Sie den EZ Setup-Assistenten:**

1. Wählen Sie oben im Menü des Modemrouters die Option **EZ Setup** (Einfache Konfiguration) aus. Der folgende Bildschirm wird angezeigt:


Setup-Assistent
Weiter
Automatische Erkennung Verbindungstyp
Der Setup-Assistent kann den Typ Ihrer Internetverbindung erkennen.
Soll der Setup-Assistent jetzt versuchen, den Verbindungstyp zu erkennen?
Ja .
Nein. Ich möchte den Router selbst einrichten.

2. Wählen Sie entweder **Yes** (Ja) oder **No, I want to configure the router myself** (Nein. Ich möchte den Router selbst einrichten) aus. Wenn Sie **No** (Nein) wählen, fahren Sie mit *Internetkonfiguration (Grundeinstellungen)* auf Seite 27 fort.
3. Klicken Sie bei Auswahl von **Yes** (Ja) auf **Next** (Weiter).

   Bei automatischer Interneterkennung durchsucht der EZ Setup-Assistent die Internetverbindung nach Servern und Protokollen, um Ihre ISP-Konfiguration bestimmen zu können.

Der EZ Setup-Assistent kann keine Point-to-Point-Tunneling-Protocol-Verbindung (PPTP) erkennen. Falls Ihr ISP PPTP verwendet, müssen Sie Ihre Internetverbindung über den unter *Internetkonfiguration (Grundeinstellungen)* auf Seite 27 beschriebenen Bildschirm einrichten.

➢ **So beheben Sie Fehler bei einer nicht erfolgreichen Internetverbindung:**

1. Überprüfen Sie sämtliche Einstellungen, um sicherzustellen, dass Sie die richtigen Optionen gewählt und alles korrekt eingegeben haben.
2. Wenden Sie sich an Ihren Provider und vergewissern Sie sich, dass Ihnen die richtigen Konfigurationsdaten vorliegen.
3. Lesen Sie den Abschnitt *Kapitel 8, Fehlerbehebung*. Falls die Probleme weiterhin bestehen, registrieren Sie Ihr Produkt, und wenden Sie sich an den technischen Support.
4. Falls Sie keine Verbindung zum Modemrouter herstellen können, überprüfen Sie die Eigenschaften des Internetprotokolls (TCP/IP) der Netzwerkverbindung in der Systemsteuerung Ihres Windows Computers. Stellen Sie dort sicher, dass Ihr Computer IP-Adresse *und* DNS-Server-Adresse automatisch bezieht. Weitere Informationen finden Sie in der Dokumentation Ihres Computers.

Herstellen einer Verbindung mit einem WLAN-Netzwerk

Wählen Sie entweder die WPS-Methode oder die manuelle Methode, um eine Verbindung mit dem WLAN-Netzwerk herzustellen.

WPS-Methode

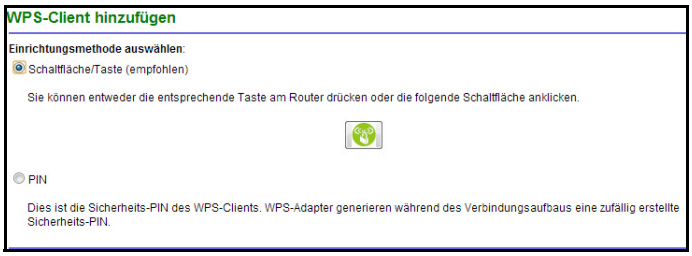
Mit WPS (Wi-Fi Protected Setup) können Sie eine Verbindung mit einem sicheren WLAN-Netzwerk herstellen, ohne das Passwort einzugeben. Stattdessen drücken Sie eine Taste oder geben eine PIN ein. Einige ältere WLAN-Geräte sind nicht zu WPS kompatibel. WPS kann nur mit den Sicherheitsoptionen WPA2 oder WPA verwendet werden.

➢ **So verwenden Sie die WPS-Taste am Modemrouter:**

1. Drücken Sie die **WPS**-Taste auf der Vorderseite des Modemrouters.
2. Wenden Sie innerhalb von 2 Minuten eine der folgenden Methoden an, um eine Verbindung über WPS mit dem Netzwerk herzustellen:
   - Wenn der Computer oder das Wireless-Gerät über eine WPS-Taste verfügt, drücken Sie diese.
   - Wählen Sie auf dem Computer oder Wireless-Gerät in der Software, mit der Sie eine Verbindung mit WLAN-Netzwerken herstellen, die **WPS**-Option aus. Befolgen Sie dann die Anweisungen zur Verbindungsherstellung.

➢ **So verwenden Sie die WPS-Methode, wenn Sie am Modemrouter angemeldet sind:**

1. Wählen Sie **Home** (Start) > **WPS Setup** (WPS-Konfiguration).
2. Klicken Sie auf **Next** (Weiter). Auf dem folgenden Bildschirm können Sie die Methode zum Hinzufügen des WPS-Clients auswählen.


WPS-Client hinzufügen
Einrichtungsmethode auswählen:
Schaltfläche/Taste (empfohlen)
Sie können entweder die entsprechende Taste am Router drücken oder die folgende Schaltfläche anklicken.
PIN
Dies ist die Sicherheits-PIN des WPS-Clients. WPS-Adapter generieren während des Verbindungsaufbaus eine zufällig erstellte Sicherheits-PIN.

3. Wählen Sie **Push Button** (Schaltfläche/Taste) oder **PIN Number** (PIN) aus. Bei jeder der Methoden versucht der Modemrouter, mit dem Computer oder Gerät zu kommunizieren, die Wireless-Sicherheit für das Gerät einzurichten und ihm zu erlauben, sich mit dem Netzwerk zu verbinden.
4. Geben Sie die Sicherheits-PIN des Clients ein, wenn der Bildschirm für die PIN-Methode angezeigt wird.

Wenn der Modemrouter eine WPS-Verbindung herstellt, wird auf dem WPS-Bildschirm des Modemrouters eine Bestätigungsmeldung angezeigt.

Manuelle Methode

Bei der manuellen Methode wählen Sie das gewünschte Netzwerk aus und geben das zugehörige Passwort ein, um eine Verbindung herzustellen.

➢ **So stellen Sie manuell eine Verbindung her:**

1. Starten Sie auf dem Computer oder Wireless-Gerät die Software, mit der die WLAN-Verbindungen verwaltet werden. Diese Software sucht nach allen verfügbaren Wireless-Netzwerken in Ihrer Umgebung.
2. Suchen Sie Ihr Netzwerk, und wählen Sie es aus.

   Der eindeutige WLAN-Netzwerkname (SSID) und das Password sind auf dem Routeretikett angegeben. Wenn Sie diese Einstellungen geändert haben, suchen Sie den Netzwerknamen, den Sie verwendet haben.
3. Geben Sie das Modemrouter-Kennwort ein, und klicken Sie auf **Connect** (Verbinden).

Modemrouter Konfiguration

3

Optionen auf der Registerkarte **Setup** (Konfiguration)

Dieses Kapitel enthält die folgenden Abschnitte:

- *Internetkonfiguration (Grundeinstellungen)*
- *ADSL-Einstellungen*
- *Voreingestellte Sicherheit*
- *Grundlagen der WLAN-Sicherheit*
- *WLAN-Konfiguration*
- *Gastnetzwerk*
- *WAN-Konfiguration*
- *LAN Setup (LAN Konfigurieren)*
- *QoS (Quality of Service)-Konfiguration*

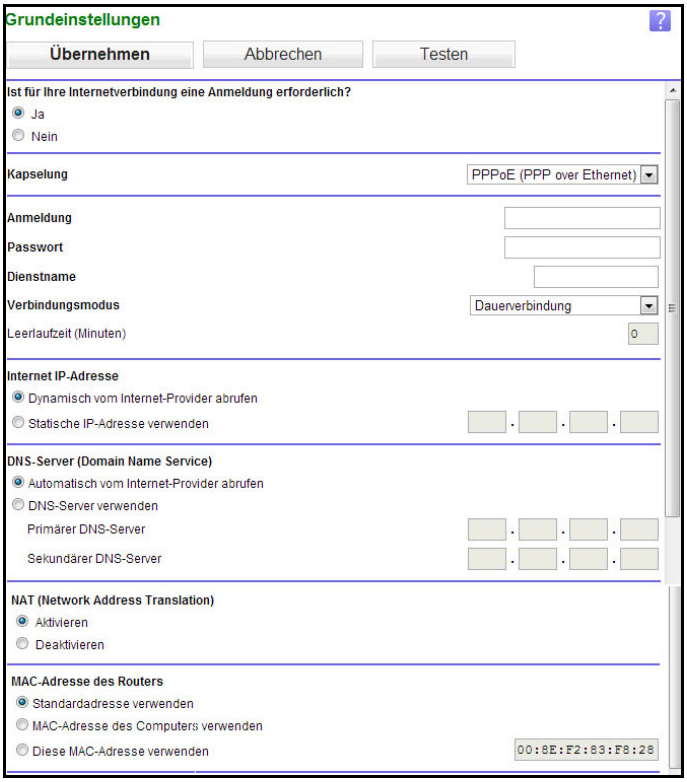
Internetkonfiguration (Grundeinstellungen)

Der Bildschirm **Basic Settings** (Grundeinstellungen) wird angezeigt, wenn Sie im EZ Setup-Assistenten die Option No**, I want to configure the Router myself** (Nein. Ich möchte den Router selbst einrichten) wählen. Er kann auch im Menü des Modemrouters aufgerufen werden. Hier können Sie ISP-Informationen anzeigen und ändern. Je nachdem, ob Ihre Internetverbindung eine Anmeldung erfordert, werden unterschiedliche Felder angezeigt.

Hinweis: Überprüfen Sie, ob das Land eingestellt ist , bevor Sie mit der manuellen Konfiguration fortfahren.

➢ **So konfigurieren Sie die Internetverbindung manuell:**

1. Wählen Sie **Setup** (Konfiguration) **> Internet Setup** (Internetkonfiguration).



2. Wählen Sie abhängig davon, ob Ihr ISP eine Anmeldung erfordert, **Yes** (Ja) oder **No** (Nein).
   - **Yes** (Ja): Wählen Sie die Verkapselungsmethode aus, und geben Sie den Anmeldenamen ein. Wenn Sie die Zeitüberschreitung für die Anmeldung ändern möchten, geben Sie einen neuen Wert in Minuten ein.
   - **No** (Nein): Geben Sie den Konto- und Domainnamen ein (falls erforderlich).

3. Geben Sie die Einstellungen für die IP-Adresse und den DNS-Server ein. Normalerweise können Sie die DSL-Standardeinstellungen beibehalten. Falls Probleme bei der Verbindungsherstellung auftreten, überprüfen Sie die ISP-Einstellungen.
4. Falls keine Anmeldung erforderlich ist, können Sie die Einstellung der MAC-Adresse vornehmen.
5. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.
6. Klicken Sie auf **Test** (Testen), um die Internetverbindung zu testen. Wenn innerhalb einer Minute keine Verbindung hergestellt werden kann, lesen Sie die Informationen unter *Kapitel 8, Fehlerbehebung*.

In den folgenden Beschreibungen werden alle verfügbaren Felder auf dem Bildschirm **Basic Settings** (Grundeinstellungen) erläutert. Welche Felder auf diesem Bildschirm angezeigt werden, ist davon abhängig, ob eine Anmeldung beim ISP erforderlich ist.

Does Your ISP Require a Login? (Ist eine Anmeldung bei Ihrem ISP erforderlich?) Antworten Sie mit **Yes** (Ja) oder **No** (Nein).

- *Ist keine Anmeldung erforderlich, werden diese Felder angezeigt:*

  Account Name (If required) (Kontoname [falls erforderlich]): Geben Sie den Kontonamen ein, den Sie von Ihrem ISP erhalten haben. Möglicherweise wird er auch als Hostname bezeichnet.

  Domain Name (If required) (Domainname [falls erforderlich]): Geben Sie den Domainnamen ein, den Sie von Ihrem ISP erhalten haben.

- *Erfordert Ihr ISP eine Anmeldung, so werden diese Felder angezeigt:*

  Encapsulation (Kapselung): Kapselung ist eine Methode zum Einschluss mehrerer Protokolle. PPP steht für Point-to-Point-Protokoll. Die Auswahlmöglichkeiten sind PPPoE (PPP over Ethernet) und PPPoA (PPP over ATM).

  Login (Anmeldung): Der Anmeldename, den Sie von Ihrem ISP erhalten haben. Dabei handelt es sich oft um eine E-Mail-Adresse.

  Password (Passwort**)**: Das Passwort, mit dem Sie sich bei Ihrem ISP anmelden.

  Service Name (If Required) (Dienstname [Falls erforderlich]): Geben Sie den Kontonamen ein, den Sie von Ihrem ISP erhalten haben. Möglicherweise wird er auch als Hostname bezeichnet.

  Connection Mode (Verbindungsmodus): Standardmäßig wird die Einstellung **Always On** (Immer zulassen) benutzt, damit der Modemrouter automatisch eine Verbindung zum Internet aufbaut.

  Idle Timeout (In minutes) (Leerlaufzeit [Minuten]): Wenn Sie die Zeitüberschreitung für die Anmeldung ändern möchten, geben Sie einen neuen Wert in Minuten ein. Dadurch wird festgelegt, wie lange der Modemrouter die Internetverbindung aktiv aufrecht erhält, nachdem die letzte Internetaktivität über das LAN verzeichnet wurde. Bei Eingabe des Werts 0 (null) werden Sie nie abgemeldet.

Internet IP Address (Internet IP-Adresse)

- **Get Dynamically from ISP** (Dynamisch vom Internet-Provider abrufen): Der ISP verwendet DHCP, um Ihnen Ihre IP-Adresse zuzuweisen. Der ISP weist diese Adressen automatisch zu.
- **Use Static IP-Address** (Statische IP-Adresse verwenden): Geben Sie die IP-Adresse, IP-Subnetzmaske und Gateway IP-Adresse ein, die Ihr ISP Ihnen zugewiesen hat. Das Gateway ist der Modemrouter des ISP, mit dem Ihr Modemrouter eine Verbindung herstellt.

Domain Name Server (DNS) Address (DNS-Server [Domain Name Service]): Jedem Domainnamen im Internet ist eine IP-Nummer zugeordnet, die der Webbrowser zum Anzeigen der entsprechenden Websites benötigt und die er über einen DNS-Server (Domain Name Service) abruft.

- **Get Automatically from ISP** (Automatisch vom ISP beziehen): Der ISP verwendet DHCP, um Ihnen DNS-Server zuzuweisen. Der ISP weist diese Adresse automatisch zu.
- **Use These DNS Servers** (DNS-Server verwenden): Wenn Sie wissen, dass Ihr ISP die DNS-Adressen während der Anmeldung nicht automatisch an den Modemrouter überträgt, wählen Sie diese Option aus, und geben Sie die IP-Adresse des primären DNS-Servers des ISPs ein. Falls außerdem die Adresse eines sekundären DNS-Servers bekannt ist, geben Sie diese ebenfalls ein.

NAT (Network Address Translation): Sie können NAT aktivieren oder deaktivieren. Wenn Sie NAT deaktivieren, können Sie auch die Firewall deaktivieren. Die Firewall kann nicht deaktiviert sein, wenn NAT aktiviert ist.

Bei Auswahl der Option für sicheres NAT werden die Computer im LAN durch eine sichere Firewall vor Angriffen aus dem Internet geschützt. Allerdings kann dies dazu führen, dass einige Online-Spiele, Point-to-Point-Anwendungen und Multimedia-Anwendungen nicht funktionieren. Bei Auswahl der Option für offenes NAT ist die Firewall nicht so sicher, es können jedoch fast alle Internetanwendungen ausgeführt werden.

Router MAC Address (MAC-Adresse des Routers): Die vom Modemrouter verwendete Netzwerk-MAC-Adresse für den Internet-Port. Einige ISPs registrieren die MAC-Adresse der Netzwerkkarte bei der Einrichtung des Kontos auf dem Computer. Danach akzeptieren sie nur Datenverkehr von der MAC-Adresse dieses Computers. Diese Funktion ermöglicht dem Modemrouter die Verwendung der MAC-Adresse Ihres Computers. (Dies wird auch als Klonen bezeichnet.)

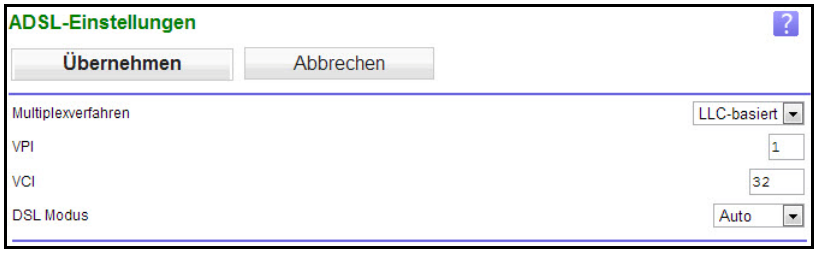
- **Use Default Address** (Standardadresse verwenden): Die Standard-MAC-Adresse wird verwendet.
- **Use Computer MAC Address** (MAC-Adresse des Computers verwenden): Der Modemrouter erfasst und verwendet die MAC-Adresse des aktuell verwendeten Computers. Verwenden Sie also den Computer, der beim ISP zugelassen ist.
- **Use This MAC Address** (Diese MAC-Adresse verwenden): Geben Sie die MAC-Adresse ein, die verwendet werden soll.

ADSL-Einstellungen

Die DSL-Einstellungen Ihres Wireless-Modemrouter funktionieren bei den meisten ISPs. Manche ISPs verwenden allerdings ein Multiplexverfahren mit virtueller Verbindungsnummer für den VPI (Virtual Path Identifier) und den VCI (Virtual Channel Identifier).

➢ **Falls Ihr ISP Ihnen ein Multiplexverfahren oder eine VPI- und VCI-Nummer zur Verfügung gestellt hat, rufen Sie die Einstellung auf:**

1. Klicken Sie auf **Setup** (Konfiguration) > **ADSL-Settings** (ADSL-Einstellungen):



2. Wählen Sie in der Dropdown-Liste **Multiplexing Method** (Multiplexverfahren) die Option **LLC-based** (LLC-basiert) oder **VC-based** (VC-basiert).
3. Geben Sie als VPI-Parameter (Virtual Path Identifier, VPI) eine Nummer zwischen 0 und 255 ein. Die Standardzahlen sind 8 für die US- Version, 0 für die weltweite Version und 1 für die deutsche Version.
4. Geben Sie als VCI-Parameter (Virtual Channel Identifier, VCI) eine Nummer zwischen 32 und 65535 ein. Die Standardzahlen sind 35 für die US- Version, 38 für die weltweite Version und 32 für die deutsche Version.
5. Als DSL Modus empfiehlt On Networks die Standardeinstellung **Auto**. Im Auto-Modus wählt das Modem die beste Modulation für Sie aus.

- Klicken Sie auf **Apply** (Übernehmen).

Voreingestellte Sicherheit

Der Modemrouter verfügt über voreingestellte Sicherheitsfunktionen. Dies bedeutet, dass der WLAN-Netzwerkname (SSID), die Passphrase und die Sicherheitsoption (Verschlüsselungsprotokoll) bereits vor der Auslieferung eingestellt werden. Die voreingestellte SSID und die voreingestellte Passphrase befinden sich an der Unterseite des Geräts.

- **Wi-Fi Network Name (SSID)** (WLAN-Netzwerkname [SSID]) bezeichnet Ihr Netzwerk, damit es von Geräten gefunden werden kann.
- **WiFi Network Password (Network Key)** (WLAN-Netzwerkpasswort [Netzwerkschlüssel]) steuert den Zugriff auf das Internet. Geräte, denen SSID und Passphrase bekannt sind, können Ihr WLAN-Netzwerk finden und eine Verbindung damit herstellen.

Hinweis: Die voreingestellte SSID und die voreingestellte Passphrase werden speziell für jedes Gerät erstellt, um Ihre Wireless-Sicherheit zu schützen und zu maximieren.

- **Security option** (Sicherheitsoption) bezeichnet die Art des Sicherheitsprotokolls für das WLAN. Mit dem angewendeten Sicherheitsprotokoll wird die Datenübertragung verschlüsselt, und es wird sichergestellt, dass nur vertrauenswürdige Geräte eine Autorisierung zur Verbindung mit dem Netzwerk erhalten. Bei der Option zur Sicherheitsvoreinstellung handelt es sich um den gemischten Modus aus WPA-PSK/WPA2-PSK, siehe *WLAN-Sicherheitsoptionen* auf Seite 32.

Auf dem Bildschirm **Wireless Settings** (Wireless-Konfiguration) können Sie die voreingestellten Sicherheitseinstellungen anzeigen und bearbeiten. Wenn Sie die voreingestellten Sicherheitseinstellungen dennoch ändern, notieren Sie die neuen Einstellungen, und bewahren Sie sie an einem sicheren Ort auf, an dem Sie sie problemlos wieder finden.

Grundlagen der WLAN-Sicherheit

Anders als bei kabelgebundenen Netzwerken können drahtlos übertragene Daten auch von außerhalb mit jedem beliebigen Gerät empfangen werden, das über einen kompatiblen Wireless-Adapter (Funkgerät) verfügt. Daher ist es sehr wichtig, dass Sie die voreingestellten Sicherheitseinstellungen beibehalten und die anderen verfügbaren Sicherheitsfunktionen verstehen. Abgesehen von den im vorigen Abschnitt beschriebenen voreingestellten Sicherheitseinstellungen verfügt Ihr Modemrouter über die hier und in *Kapitel 4, Sicherheitseinstellungen* beschriebenen Sicherheitsfunktionen.

- Wireless-Verbindung abschalten
- SSID-Broadcast deaktivieren
- Einschränkung des Zugriffs über MAC-Adressen
- Wireless-Sicherheitsoptionen

SSID-Broadcast deaktivieren

Standardmäßig sendet der Modemrouter seinen WLAN-Netzwerknamen (SSID), damit er von Geräten gefunden werden kann. Wenn Sie diese Einstellung ändern, sodass das Versenden nicht zugelassen wird, können Wireless-Geräte Ihren Modemrouter erst finden, wenn sie mit der gleichen SSID konfiguriert werden.

Hinweis: Durch das Abschalten von SSID-Broadcast wird die „Entdeckungsfunktion“ für WLAN-Netzwerke von Produkten wie Windows XP außer Betrieb gesetzt, doch die Daten sind immer noch ungeschützt gegen hartnäckige Schnüffler, die spezielle Software wie Wireless Sniffer einsetzen. Wenn Sie das Versenden zulassen, stellen Sie sicher, dass die Wireless-Sicherheit aktiviert ist.

Einschränkung des Zugriffs über MAC-Adressen

Sie können Ihre Netzwerksicherheit erhöhen, indem Sie nur bestimmten Computern den Zugriff über ihre MAC-Adressen (Media Access Control) gewähren. Sie können den Zugriff auf bekannte PCs beschränken, damit unbekannte Computer keine drahtlose Verbindung zum Modemrouter aufbauen können. Die Filterung der MAC-Adressen der WLAN-Geräte fügt der bereits aktivierten WLAN-Sicherheitsoption noch zusätzlichen Schutz hinzu. Die Liste der zugriffsberechtigten Geräte legt anhand der MAC-Adressen fest, welche Wireless-Hardwaregeräte mit dem Modemrouter in Verbindung treten dürfen. Die entsprechende Vorgehensweise finden Sie unter *Erweiterte WLAN-Konfiguration* auf Seite 76.

WLAN-Sicherheitsoptionen

Eine Sicherheitsoption bezeichnet die Art des Sicherheitsprotokolls für das WLAN. Mit dem Sicherheitsprotokoll wird die Datenübertragung verschlüsselt, und es wird sichergestellt, dass nur vertrauenswürdige Geräte eine Autorisierung zur Verbindung mit dem Netzwerk erhalten. Es gibt diverse Verschlüsselungsmethoden: Wi-Fi Protected Access II (WPA2), WPA und Wired Equivalent Privacy (WEP). WPA2 ist die neueste und sicherste Methode und wird empfohlen, sofern Ihre Geräte sie unterstützen. WPA verfügt über mehrere Optionen, z. B. PSK-Verschlüsselung (Pre-Shared Key) und 802.1x-Verschlüsselung für Unternehmen. Die WLAN-Sicherheitseinstellungen können deaktiviert werden, dies wird jedoch nicht empfohlen. Sie können die WLAN-Sicherheitsoptionen im Bildschirm **Wireless Settings** (Wireless-Konfiguration) anzeigen und bearbeiten. Siehe *WLAN-Konfiguration* auf Seite 32.

WLAN-Konfiguration

Im Bildschirm **Wireless Settings** (Wireless-Konfiguration) können Sie die Einstellungen des WLAN-Netzwerks anzeigen oder konfigurieren. Ihr voreingestellter Modemrouter verfügt über einen eindeutigen Netzwerknamen und ein eindeutiges Passwort. Diese befinden sich auf dem Produktetikett. Falls Sie sich entschließen, sie zu ändern, notieren Sie bitte die neuen Einstellungen, und bewahren Sie sie an einem sicheren Ort auf.

Wenn Sie einen WLAN-Computer zur Änderung des WLAN-Netzwerknamens (SSID) oder anderer Sicherheitsoptionen verwenden, wird die Verbindung getrennt, wenn Sie auf **Apply** (Übernehmen) klicken. Verwenden Sie einen Computer mit Kabelverbindung für den Zugriff auf den Modemrouter, um dieses Problem zu umgehen.

Überprüfen jedes Geräts in Ihrem Netzwerk

Überprüfen Sie Folgendes, bevor Sie beginnen:

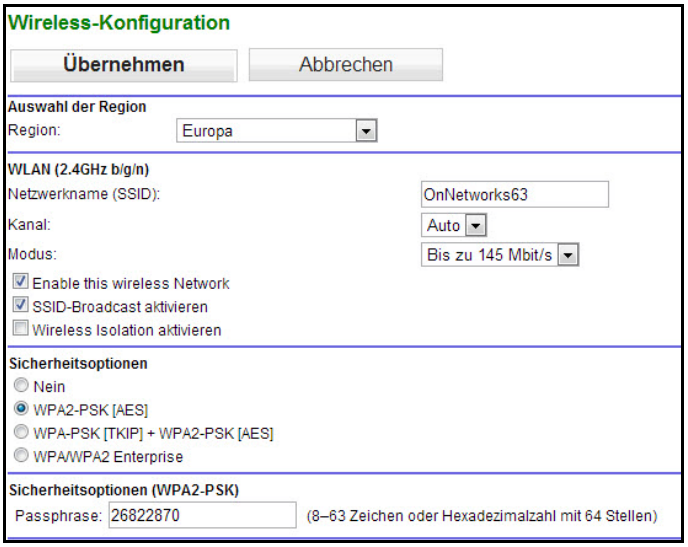
- Jeder WLAN-Computer muss in der Lage sein, eine IP-Adresse über DHCP vom Modemrouter zu beziehen, wie in *Verwenden der Standard-TCP/IP-Eigenschaften für DHCP* auf Seite 19 beschrieben.
- Jeder Computer oder WLAN-Adapter in Ihrem Netzwerk muss die gleiche SSID und den gleichen WLAN-Modus (Bandbreite/Übertragungsrate) aufweisen wie der Modemrouter. Überprüfen Sie, ob die Wireless-Adapter der einzelnen Computer die von Ihnen ausgewählten Modus- und Sicherheitsoptionen unterstützen.
- Die Sicherheitsoption auf jedem Wireless-Gerät im Netzwerk muss zumModemrouter passen. Wenn Sie beispielsweise eine Sicherheitsoption wählen, die eine Passphrase erfordert, verwenden Sie bitte unbedingt die gleiche Passphrase für jeden WLAN-Computer im Netzwerk.

Wireless-Konfiguration anzeigen und bearbeiten

Ihr voreingestellter Modemrouter wird mit einem eindeutigen WLAN-Netzwerknamen (SSID) und einem eindeutigen Netzwerkpasswort geliefert. Diese Informationen sind auf das Etikett Ihres Modemrouters aufgedruckt. Sie können diese Einstellungen mithilfe des Bildschirms **Wireless Settings** (Wireless-Konfiguration) anzeigen und bearbeiten.

➢ **So zeigen Sie die Wireless-Konfiguration an oder ändern sie:**

1. Wählen Sie **Setup** (Konfiguration) > **Wireless Settings** (Wireless-Konfiguration). Der folgende Bildschirm wird angezeigt.



2. Nehmen Sie alle erforderlichen Änderungen vor, und klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

> **Hinweis:** Die Abschnitte, Einstellungen und Vorgehensweisen dieses Bildschirms werden im Folgenden erläutert.

3. Konfigurieren und testen Sie die Wireless-Verbindung Ihrer Computer.
   a. Verwenden Sie Ihren Wireless-Computer bzw. Ihr Wireless-Gerät, um eine Verbindung mit dem Netzwerk herzustellen. Geben Sie bei Aufforderung das Netzwerkpasswort ein.
   b. Stellen Sie bei einem drahtlos verbundenen Computer sicher, dass Sie auf das Internet zugreifen können.

Felder auf dem Bildschirm **Wireless Settings** (Wireless-Konfiguration)

- **Enable SSID Broadcast** (SSID-Broadcast aktivieren): Diese Einstellung ermöglicht die Übertragung der SSID des Modemrouters, damit WLAN-Geräte diesen WLAN-Namen (SSID) in ihrer Liste der gescannten Netzwerke anzeigen können. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **Apply** (Übernehmen), um die SSID-Übertragung zu deaktivieren.
- **Name (SSID)** (Netzwerkname [SSID]): Die SSID wird auch als Netzwerkname bezeichnet. Geben Sie einen (maximal) 32 Zeichen langen Namen in dieses Feld ein. Bei diesem Feld wird zwischen Groß- und Kleinschreibung unterschieden. Die standardmäßige SSID wird nach dem Zufallsprinzip generiert und muss normalerweise nicht geändert werden.
- **Region**: Der Ort, an dem der Modemrouter verwendet wird. Wenn Sie den Modemrouter in einer anderen Region als den hier aufgelisteten betreiben, verstoßen Sie möglicherweise gegen gesetzliche Bestimmungen.
- **Channel** (Kanal): Der Funkkanal, der von Gateway 1 bis 13 verwendet wird. Ändern Sie den Kanal nicht, es sei denn, es treten Funkstörungen auf (was sich durch abgebrochene Verbindungen und/oder langsame Datenübertragung zeigt). Testen Sie in diesem Fall verschiedene Kanäle, um den optimalen Kanal zu finden.
- **Mode** (Modus): Die Standardeinstellung **Up to 145 Mbps** (Bis zu 145 MBit/s) ermöglicht WLAN-Geräten der Standards 802.11n und 802.11g die Verbindung mit dem Netzwerk. g und b unterstützen bis zu 54 MBit/s. **Up to 300 Mbps** (Bis zu 300 MBit/s) unterstützt bis zu 300 MBit/s.

Konfiguration der Sicherheitsoptionen

Im Abschnitt **Security Options** (Sicherheitsoptionen) auf dem Bildschirm **Wireless Settings** (Wireless-Konfiguration) können Sie die Sicherheitsoption und die Passphrase ändern. Auf dem Modemrouter sind bereits WPA2 und WPA konfiguriert. Weitere Informationen zum Ändern dieser Einstellungen finden Sie im folgenden Abschnitt, *Ändern der WPA-Sicherheitsoption und Passphrase*.

Ändern der WPA-Sicherheitsoption und Passphrase

➢ **So ändern Sie die WPA-Sicherheitsoption:**

1. Wählen Sie im Abschnitt **Security options** (Sicherheitsoptionen) die gewünschte WPA-Option.

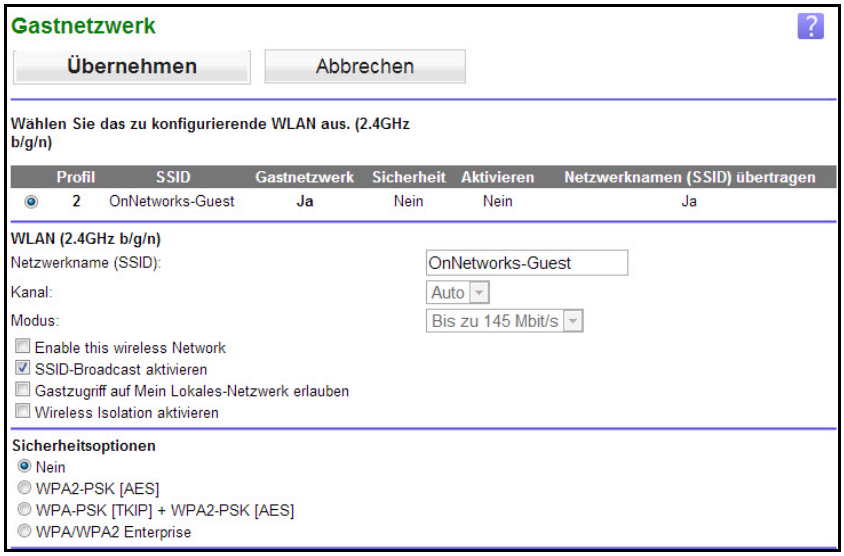
2. Geben Sie die Passphrase ein, die verwendet werden soll. Dabei handelt es sich um eine Textzeichenfolge mit einer Länge von 8 bis 63 Zeichen.
3. Klicken Sie auf **Apply** (Übernehmen).

Gastnetzwerk

Sie können ein Gastnetzwerk einrichten, damit Besucher Ihre Internetverbindung verwenden können.

➢ **So richten Sie ein Gastnetzwerk ein:**

1. Wählen Sie **Basic** (Grundeinstellungen) > **Guest** (Gast).



2. Aktivieren Sie die Kontrollkästchen und Optionsschaltflächen zum Festlegen der Einstellungen Ihres Gastnetzwerks.

   Die Einstellungen gleichen den Einstellungen des Bildschirms zur Wireless-Konfiguration. Siehe *WLAN-Konfiguration* auf Seite 32.

3. Klicken Sie auf **Apply** (Übernehmen).

WAN-Konfiguration

Mit dem Bildschirm **WAN Setup** (WAN-Konfiguration) können Sie einen DMZ-Server (Demilitarized Zone; entmilitarisierte Zone) konfigurieren, die MTU-Größe (Maximum Transmit Unit) ändern und den Modemrouter so einrichten, dass er auf Ping-Anforderungen am WAN (Internet)-Port reagiert. Wählen Sie **Setup** (Konfiguration) > **Internet Port** (Internet-Port) aus. Der folgende Bildschirm wird geöffnet:

- **Disable Port Scan and DoS Protection** (Schutz vor Port-Abfragen und DoS-Angriffen deaktivieren): Der Schutz vor DoS schützt Ihr LAN vor Denial of Service-Angriffen wie SYN-Floods, Smurf-Angriffen, Ping of Death, Teardrop-Angriffen, UDP-Floods, ARP-Angriffen, Spoofing (ICMP), Null-Scans u. a. Diese Option sollte nur deaktiviert werden, wenn dies aus gegebenem Anlass erforderlich ist.
- **Default DMZ Server** (DMZ-Standardserver): Diese Funktion kann beim Spielen von Online-Spielen oder bei Videokonferenzen hilfreich sein. Seien Sie vorsichtig bei Verwendung dieser Funktion, da die Firewall-Sicherheitseinstellungen dadurch weniger effektiv sind. Weitere Informationen finden Sie im folgenden Abschnitt, *DMZ-Standardserver*.
- **Respond to Ping on Internet Port** (Auf Ping-Anforderungen am Internet-Port reagieren): Aktivieren Sie dieses Kontrollkästchen, wenn der Modemrouter auf Ping-Anforderungen aus dem Internet reagieren soll. Diese Option sollte nur für Diagnosezwecke verwendet werden, da Ihr Modemrouter dadurch entdeckt werden kann. Aktivieren Sie dieses Kästchen nur, wenn ein dringender Grund dazu vorliegt.
- **MTU Size (in bytes)** (MTU-Größe [in Byte]): Der MTU-Wert (Maximum Transmit Unit) beträgt normalerweise 1500 Byte für lokale Netzwerke und 1492 Byte für PPPoE-Verbindungen. Bei einigen ISPs muss ein niedrigerer MTU-Wert eingestellt werden. Dies ist nur selten erforderlich. Reduzieren Sie den MTU-Wert nur, wenn dies für Ihre ISP-Verbindung tatsächlich erforderlich ist. Siehe *Ändern der MTU-Größe* auf Seite 37.
- **NAT Filtering** (NAT-Filter): NAT (Network Address Translation) legt fest, wie eingehender Datenverkehr vom Modemrouter verarbeitet wird. Bei Auswahl der Option für sicheres NAT werden die Computer im LAN durch eine sichere Firewall vor Angriffen aus dem Internet geschützt. Allerdings kann dies dazu führen, dass einige Online-Spiele, Point-to-Point-Anwendungen und Multimedia-Anwendungen nicht funktionieren. Bei

Auswahl der Option für offenes NAT ist die Firewall nicht so sicher, es können jedoch fast alle Internetanwendungen ausgeführt werden.

- **Disable SIP ALG** (SIP ALG deaktivieren): Zur Optimierung von VoIP-Anrufen, die das SIP (Session Initiation Protocol) verwenden, ist standardmäßig ein SIP Application Level Gateway (ALG) aktiviert. Aktivieren Sie das Kontrollkästchen **Disable SIP ALG** (SIP ALG deaktivieren), um das SIP ALG zu deaktivieren. Die Deaktivierung des SIP ALG kann bei der Ausführung bestimmter Anwendungen sinnvoll sein.

DMZ-Standardserver

Der DMZ-Standardserver kann bei Online-Spielen und Videokonferenz-Anwendungen, die nicht zu NAT (Network Address Translation) kompatibel sind, hilfreich sein. Der Modemrouter ist darauf programmiert, einige dieser Anwendungen zu erkennen und zu unterstützen, doch bei anderen Anwendungen können Probleme auftreten. In einigen Fällen ist es möglich, die Anwendung auf einem lokalen Computer fehlerfrei auszuführen, wenn die IP-Adresse des Computers als DMZ-Standardserver eingegeben wird.

WARNUNG:

DMZ-Server stellen ein Sicherheitsrisiko dar. Ein Computer, der als DMZ-Standardserver festgelegt wird, verliert einen Großteil des Firewall-Schutzes und ist Angriffen aus dem Internet ausgesetzt. Dies kann dazu führen, dass der DMZ-Server-Computer für Angriffe auf andere Computer in Ihrem Netzwerk verwendet wird.

Über das Internet eingehende Daten werden normalerweise vom Router zurückgewiesen, wenn sie nicht von einem Ihrer lokalen Computer angefordert wurden oder zu einem der im Bildschirm **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) konfigurierten Dienste gehören. Statt diese Daten zurückzuweisen, können Sie sie vom Router an einen Computer in Ihrem Netzwerk weiterleiten. Dieser Computer ist der DMZ-Standardserver.

➢ **So richten Sie einen DMZ-Standardserver ein:**

1. Aktivieren Sie auf dem Bildschirm **WAN Setup** (WAN-Konfiguration) das Kontrollkästchen **Default DMZ Server** (DMZ-Standardserver).
2. Geben Sie die IP-Adresse ein.
3. Klicken Sie auf **Apply** (Übernehmen).

Ändern der MTU-Größe

Die MTU (Maximum Transmission Unit) ist das größte Datenpaket, das in einem Netzwerk übertragen wird. Wenn ein Netzwerkgerät über das Internet mit einem anderen Netzwerkgerät Daten austauscht, wandert das Datenpaket dabei über viele Geräte. Weist eines der Geräte im Datenpfad eine niedrigere MTU-Einstellung als die anderen Geräte auf,

müssen die Datenpakete aufgeteilt oder „fragmentiert“ werden, damit auch das Gerät mit dem niedrigsten MTU-Wert die Daten weitersenden kann.

Die beste MTU-Einstellung für On Networks-Geräte ist oft die Standardeinstellung. Durch eine Änderung des Werts wird manchmal nur ein Problem behoben und dafür ein zusätzliches Problem geschaffen. Ändern Sie die MTU nur, wenn eine der folgenden Situationen eintritt:

- Sie können keine Verbindung mit Ihrem ISP oder einem anderen Internetdienst herstellen, und der technische Support des ISP oder On Networks empfiehlt eine Änderung der MTU-Einstellung. Für folgende webbasierte Anwendungen muss die MTU möglicherweise geändert werden:
  - Eine sichere Website, die nicht geöffnet werden kann oder eine Webseite nur zum Teil anzeigt
  - Yahoo!-E-Mail
  - MSN-Portal
  - DSL-Dienst von AOL
- Sie verwenden VPN und haben mit erheblichen Leistungsproblemen zu kämpfen.
- Sie haben zur Erhöhung der Leistung ein Programm für die MTU-Optimierung eingesetzt und haben nun Probleme mit der Verbindung oder Leistung.

Hinweis: Eine falsche MTU-Einstellung kann Probleme mit der Internetverbindung verursachen. Sie kann beispielsweise zur Folge haben, dass bestimmte Webseiten, Frames in Webseiten, sichere Anmeldeseiten oder FTP- oder POP-Server nicht mehr aufgerufen werden können.

Wenn Sie ein MTU-Problem vermuten, kann es häufig dadurch gelöst werden, die MTU zu 1400 zu ändern. Falls Sie verschiedene Lösungen ausprobieren möchten, können Sie die MTU nach und nach vom Maximalwert 1500 heruntersetzen, bis das Problem behoben ist. In der folgenden Tabelle werden häufige MTU-Größen und Anwendungen dargestellt.

Tabelle 2. Häufige MTU-Größen

MTU	Anwendung
1500	Die größte Netzwerkpaketgröße und der Standardwert. Dies ist die normale Einstellung für Verbindungen ohne PPPoE und VPN sowie der Standardwert für Modemrouter, Adapter und Switches von On Networks.
1492	Wird in PPPoE-Umgebungen verwendet
1472	Maximal verwendbare Größe für Ping-Anforderungen (Größere Pakete werden fragmentiert.)
1468	Wird in einigen DHCP-Umgebungen verwendet

Tabelle 2. Häufige MTU-Größen (Fortsetzung)

MTU	Anwendung
1458	Wird in PPPoA-Umgebungen verwendet
1460	Verwendbar u. a. für AOL, wenn Sie keine großen E-Mail-Anhänge senden oder empfangen
1436	Wird in PPTP-Umgebungen oder mit VPN verwendet
1400	Maximale Größe für AOL-DSL
576	Normaler Wert für DFÜ-Verbindungen

➢ **So ändern Sie die MTU-Größe:**

1. Wählen Sie **Advanced** (Erweitert) > **Setup** (Konfiguration) > **WAN Setup** (WAN-Konfiguration) aus.
2. Geben Sie in das Feld **MTU Size** (MTU-Größe) einen Wert zwischen 64 und 1500 ein.
3. Klicken Sie auf **Übernehmen** (Apply), um die Einstellungen zu speichern.

LAN Setup (LAN Konfigurieren)

Der Bildschirm **LAN Setup** (LAN Konfigurieren) ermöglicht die Konfiguration von LAN-IP-Diensten wie DHCP (Dynamic Host Configuration Protocol) und RIP (Routing Information Protocol).

Der Modemrouter wird mit einer Voreinstellung zur Verwendung privater IP-Adressen im LAN und für die Verwendung als DHCP-Server ausgeliefert. Die voreingestellte LAN-IP-Konfiguration des Modemrouters sieht wie folgt aus:

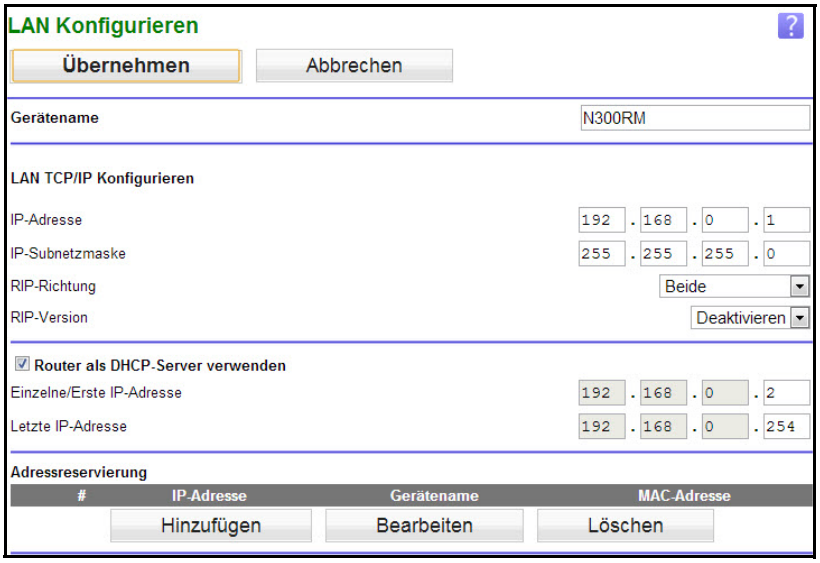
- LAN-IP-Adresse. **192.168.0.1**
- Subnetzmaske. **255.255.255.0**

Diese Adressen gehören zu dem für die Verwendung in privaten Netzwerken bestimmten privaten Adressbereich und sind für die meisten Anwendungen geeignet. Wenn für Ihr Netzwerk ein anderes IP-Adressenschema erforderlich ist, können Sie die entsprechenden Einstellungen auf dem Bildschirm **LAN Setup** (LAN Konfigurieren) vornehmen.

> **Hinweis:** *Wenn Sie die LAN-IP-Adresse des Modemrouters ändern, während Sie über den Browser verbunden sind, wird die Verbindung unterbrochen. Sie müssen dann eine Verbindung zur neuen IP-Adresse herstellen und sich erneut anmelden.*

➢ **So ändern Sie die LAN-Einstellungen:**

1. Wählen Sie **Setup** (Konfiguration) > **LAN Setup** (LAN Konfigurieren) aus, um den folgenden Bildschirm anzuzeigen:



2. Geben Sie die Einstellungen ein, die Sie anpassen möchten. Diese Einstellungen werden im folgenden Abschnitt, *LAN-TCP/IP-Konfiguration*, beschrieben.
3. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

LAN-TCP/IP-Konfiguration

- **IP Address** (IP-Adresse): Die LAN-IP-Adresse des Modemrouters
- **IP Subnet Mask** (IP-Subnetzmaske): Die LAN-Subnetzmaske des Modemrouters. Zusammen mit der IP-Adresse sorgt die IP-Subnetzmaske dafür, dass ein Gerät erkennen kann, bei welchen Adressen es sich um lokale Adressen handelt und welche Adressen nur über ein Gateway oder einen Modemrouter zu erreichen sind.
- **RIP Direction** (RIP-Richtung): Über RIP (Router Information Protocol) kann ein Router Routinginformationen mit anderen Routern austauschen. Diese Einstellung legt fest, auf welche Weise der Router RIP-Pakete sendet und empfängt. Die Standardeinstellung ist **Both** (Beide). Bei Auswahl von **Both** (Beide) oder **Out Only** (Nur abgehend) sendet der Router die Routingtabelle in regelmäßigen Abständen. Bei Auswahl von **Both** (Beide) oder **In Only** (Nur ankommend) übernimmt der Router eingehende Routinginformationen.
- **RIP Version** (RIP-Version): Mit dieser Einstellung können Sie das Format und die Broadcastmethode für den Versand von RIP-Paketen durch den Modemrouter steuern. Beim Empfang werden beide Formate erkannt. Standardmäßig ist die RIP-Funktion deaktiviert.

  RIP-1 wird praktisch von allen Netzwerkgeräten unterstützt. Es eignet sich für alle gängigen Netzwerkkonfigurationen.

Bei **RIP-2** werden mehr Informationen übertragen. Sowohl bei RIP-2B als auch bei RIP-2M werden die Routingdaten im RIP-2-Format übermittelt. Bei RIP-2B erfolgt die Übertragung mittels Subnetz-Broadcasting. Bei RIP-2M erfolgt die Übertragung mittels Multicasting.

Use Router as a DHCP Server *(Router als DHCP-Server verwenden)*

Dieses Kontrollkästchen ist standardmäßig aktiviert, damit der Modemrouter als DHCP-Server (Dynamic Host Configuration Protocol) verwendet wird.

- **Starting IP Address** (Einzelne/Erste IP-Adresse): Geben Sie den Beginn des Bereichs für den IP-Adresspool im Subnetz des Modemrouters an.
- **Ending IP Address** (Letzte IP-Adresse): Geben Sie das Ende des Bereichs für den IP-Adresspool im Subnetz des Modemrouters an.

Adressreservierung

Wenn Sie für einen Computer im LAN eine reservierte IP-Adresse angeben, wird diesem Computer bei jedem Zugriff auf den DHCP-Server des Modemrouters dieselbe IP-Adresse zugewiesen. Weisen Sie Servern, die feste IP-Einstellungen erfordern, reservierte IP-Adressen zu.

Verwenden des Modemrouters als DHCP-Server

Standardmäßig fungiert der Modemrouter als DHCP-Server. Der Router vergibt IP-, DNS-Server- und Standardgateway-Adressen an alle Computer, die mit dem LAN verbunden sind. Als Standardgateway-Adresse wird die LAN-Adresse des Modemrouters vergeben. Der Modemrouter vergibt IP-Adressen an die angeschlossenen Computer aus einer Auswahl von IP-Adressen, die auf diesem Bildschirm festgelegt werden. Jede dieser Adressen wird vor der Vergabe getestet, um doppelte Adressen im LAN zu verhindern. Für die meisten Anwendungen genügen die DHCP- und TCP/IP-Voreinstellungen des Modemrouters.

Sie können die IP-Adressen angeben, die zur Vergabe verfügbar sein sollen, indem Sie die erste und letzte IP-Adresse festlegen. Diese Adressen sollten zum selben IP-Adressen-Subnetz gehören wie die LAN-IP-Adresse des Modemrouters. Wenn Sie das Standard-Adressenschema verwenden, legen Sie einen Bereich zwischen 192.168.0.2 und 192.168.0.254 fest. Halten Sie jedoch ggf. einen Teil des Bereichs für Geräte mit festen IP-Adressen frei.

Der Modemrouter übermittelt die folgenden Parameter an jedes LAN-Gerät, das eine DHCP-Anforderung absendet:

- Eine IP-Adresse aus dem festgelegten Bereich
- Subnetzmaske
- Gateway IP-Adresse (die LAN-IP-Adresse des Modemrouters)

- Primärer DNS-Server (wenn Sie auf dem Bildschirm **Basic Settings** [Grundeinstellungen] eine primäre DNS-Adresse eingegeben haben - andernfalls die LAN-IP-Adresse des Modemrouters)
- Sekundärer DNS-Server (wenn Sie auf dem Bildschirm **Basic Settings** [Grundeinstellungen] eine sekundäre DNS-Adresse eingegeben haben)

Wenn ein anderes Gerät in Ihrem Netzwerk als DHCP-Server eingesetzt werden soll oder Sie die Netzwerkeinstellungen auf allen Computern konfigurieren möchten, deaktivieren Sie das Kontrollkästchen **Use Router as DHCP Server** (Router als DHCP-Server verwenden), und klicken Sie auf **Apply** (Übernehmen). Lassen Sie dieses Kontrollkästchen andernfalls aktiviert. Wenn dieser Dienst nicht aktiviert ist und kein anderer DHCP-Server im Netzwerk verfügbar ist, müssen Sie die IP-Adressen der Computer manuell festlegen, da Sie sonst nicht auf den Modemrouter zugreifen können.

Adressreservierung

Wenn Sie für einen Computer im LAN eine reservierte IP-Adresse angeben, wird diesem Computer bei jedem Zugriff auf den DHCP-Server des Modemrouters dieselbe IP-Adresse zugewiesen. Weisen Sie Computern oder Servern, die feste IP-Einstellungen erfordern, reservierte IP-Adressen zu.

➢ **So reservieren Sie eine IP-Adresse:**

1. Klicken Sie im Abschnitt **Address Reservation** (Adressreservierung) des Bildschirms auf die Schaltfläche **Add** (Hinzufügen).
2. Geben Sie im Feld **IP Address** (IP-Adresse) die IP-Adresse ein, die dem Computer oder Server zugewiesen werden soll. (Wählen Sie eine IP-Adresse aus dem LAN-Subnetz des Modemrouters aus, z. B. 192.168.0.x).
3. Geben Sie die MAC-Adresse des Computers oder Servers ein.

   Tipp: Wenn der Computer bereits in Ihrem Netzwerk registriert ist, können Sie seine MAC-Adresse aus dem Bildschirm **Attached Devices** (Angeschlossene Geräte) kopieren und hier einfügen.

4. Klicken Sie auf **Apply** (Übernehmen), um die reservierte Adresse in die Tabelle aufzunehmen.

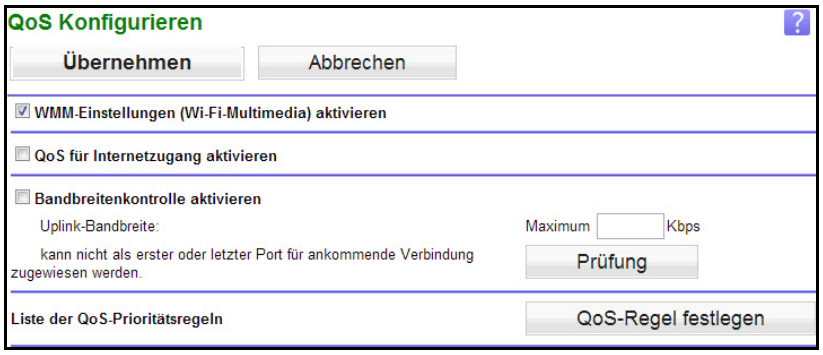
   Die reservierte Adresse wird erst zugewiesen, wenn der Computer das nächste Mal mit dem DHCP-Server des Modemrouters Kontakt aufnimmt. Starten Sie den Computer neu, oder greifen Sie auf seine IP-Konfiguration zu, und erzwingen Sie eine DHCP-Freigabe und -Erneuerung.

Um den Eintrag einer reservierten Adresse zu bearbeiten oder zu löschen, wählen Sie die Optionsschaltfläche neben der reservierten Adresse aus, die Sie bearbeiten oder löschen möchten. Klicken Sie dann auf **Edit** (Bearbeiten) oder **Delete** (Löschen).

QoS (Quality of Service)-Konfiguration

QoS ist eine erweiterte Funktion, mit der Prioritäten für verschiedene Datentypen festgelegt werden können. Der Modemrouter unterstützt QoS-Prioritätseinstellungen über das WLAN und für die Internetverbindung. Sie können QoS im Bildschirm QoS Setup (QoS Konfigurieren) einrichten.

Wählen Sie **Setup** (Konfiguration) > **QoS Setup** (QoS -Konfiguration) aus, um den folgenden Bildschirm anzuzeigen:



Aktivieren von WMM QoS für drahtlose Multimedia-Anwendungen

Der Modemrouter unterstützt WMM QoS (Wi-Fi Multimedia Quality of Service), um dem drahtlosen Sprach- und Videodatenverkehr über das WLAN Priorität einzuräumen. Mit WMM QoS erhalten drahtlose Datenpakete Priorität vor anderen Anwendungen. Die vier Zugriffskriterien lauten Sprache, Video, bester Versuch und Hintergrund. Damit eine Anwendung die Vorteile von WMM QoS nutzen kann, muss sowohl für die Anwendung als auch für den Client, auf dem die Anwendung ausgeführt wird, WMM aktiviert sein. Ältere Anwendungen, die WMM nicht unterstützen, und Anwendungen, für die QoS nicht erforderlich ist, werden der Kategorie bester Versuch zugeordnet. Diese Kategorie steht in der Prioritätsliste nach Sprache und Video.

WMM QoS ist standardmäßig aktiviert. Sie können die Option im Bildschirm **QoS Setup** (QoS Konfigurieren) deaktivieren, indem Sie das Kontrollkästchen **Enable WMM (Wi-Fi Multimedia)** (WMM-Einstellungen [Wi-Fi-Multimedia] aktivieren) deaktivieren und auf **Apply** (Übernehmen) klicken.

Konfigurieren von QoS für den Internetzugriff

Sie können den folgenden Datenverkehrstypen Vorrang beim Internetzugriff einräumen:

- Bestimmte Anwendungen
- Bestimmte Online-Spiele
- Einzelne Netzwerk-LAN-Ports des Modemrouters
- Spezifisches Gerät nach MAC-Adresse

Um die Priorität des Datenverkehrs anzugeben, müssen Sie eine Richtlinie für den Datenverkehrstyp erstellen und die Richtlinie der Tabelle mit den QoS-Richtlinien auf dem Bildschirm **QoS Setup** (QoS Konfigurieren) hinzufügen. Die Tabelle mit den QoS-Richtlinien enthält bereits viele gängige Anwendungen und Online-Spiele, deren Leistung durch die QoS-Einstellungen erhöht werden kann.

QoS für Anwendungen und Online-Spiele

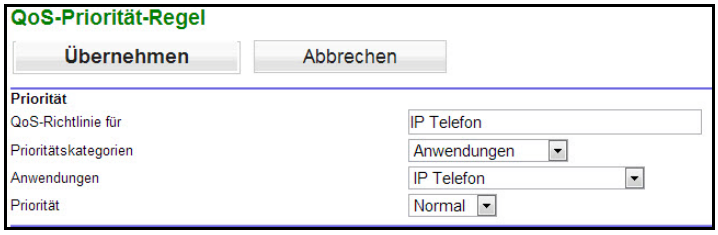
➢ **So erstellen Sie eine QoS-Richtlinie für Anwendungen und Online-Spiele:**

1. Aktivieren Sie auf dem Bildschirm **QoS Setup** (QoS Konfigurieren) das Kontrollkästchen **Turn Internet Access QoS On** (QoS für Internetzugang aktivieren).
2. Klicken Sie auf die Schaltfläche **Setup QoS Rule** (QoS-Regel festlegen), um die vorhandenen Prioritätsregeln anzuzeigen.

Liste der QoS-Prioritätsregeln
Übernehmen
Abbrechen
QoS-Richtlinie Priorität Beschreibung
1 MSN messenger Hoch MSN messenger Anwendung
2 Yahoo Messenger Hoch Yahoo Messenger Anwendung
3 IP Telefon Höchste IP Telefon Anwendung
4 Vonage IP Telefon Höchste Vonage IP Telefon Anwendung
5 NetMeeting Hoch NetMeeting Anwendung
6 AIM Hoch AIM Anwendung
7 Google Gespräch Höchste Google Gespräch Anwendung
8 Gegenschlag Hoch Online-Spiele Gegenschlag
9 Age of Empires Hoch Online-Spiele Age of Empires
10 Everquest Hoch Online-Spiele Everquest
11 Beben 2 Hoch Online-Spiele Beben 2
12 Beben 3 Hoch Online-Spiele Beben 3
13 Unreal Tournament Hoch Online-Spiele Unreal Tournament
14 Warcraft Hoch Online-Spiele Warcraft
Bearbeiten
Löschen
Alle löschen
Prioritätsregel hinzufügen

Sie können eine Regel bearbeiten oder löschen, indem Sie die entsprechende Optionsschaltfläche aktivieren und auf die Schaltfläche **Edit** (Bearbeiten) oder **Delete** (Löschen) klicken. Außerdem können Sie alle Regeln löschen, indem Sie auf die Schaltfläche **Delete All** (Alle löschen) klicken.

3. Zum Hinzufügen einer Prioritätsregel blättern Sie bis zum Ende des Bildschirms **QoS Setup** (QoS Konfigurieren), und klicken Sie auf **Add Priority Rule** (Prioritätsregel hinzufügen). Der folgende Bildschirm wird angezeigt:



4. Geben Sie in das Feld **QoS Policy for** (QoS-Richtlinie für) den Namen der Anwendung oder des Spiels ein.
5. Wählen Sie in der Liste **Priority Category** (Prioritätskategorien) entweder **Applications** (Anwendungen) oder **Online Gaming** (Online-Spiele) aus. In beiden Fällen wird eine Liste der Anwendungen oder Spiele angezeigt.
6. Sie können einen vorhandenen Eintrag aus der Liste auswählen oder blättern und **Add a New Application** (Neue Anwendung hinzufügen) bzw. **Add a New Game** (Neues Spiel hinzufügen) auswählen.

   Wenn Sie einen Eintrag hinzufügen, wird der Bildschirm **Priority Rules** (Prioritätsregeln) erweitert.

   a. Geben Sie in das Feld **QoS Policy for** (QoS-Richtlinie für) einen Namen für die neue Anwendung oder das neue Spiel ein.

   b. Wählen Sie in der Liste **Connection Type** (Verbindungstyp) entweder **TCP** oder **UDP** oder beides (**TCP/UDP**) aus. Geben Sie die Portnummer oder den Portnummernbereich für die Anwendung oder das Spiel an.
7. Wählen Sie aus der Liste **Priority** (Priorität) die Priorität aus, die dem Datenverkehr beim Internetzugriff im Vergleich zu anderen Anwendungen und Datenverkehrstypen zugeordnet werden soll. Die verfügbaren Optionen sind **Low** (Niedrig), **Normal**, **High** (Hoch) und **Highest** (Höchste).
8. Klicken Sie auf **Apply** (Übernehmen), um diese Regel in der Liste der QoS-Richtlinien zu speichern, und kehren Sie zum Bildschirm **QoS Setup** (QoS Konfigurieren) zurück.

QoS für einen Modemrouter-LAN-Port

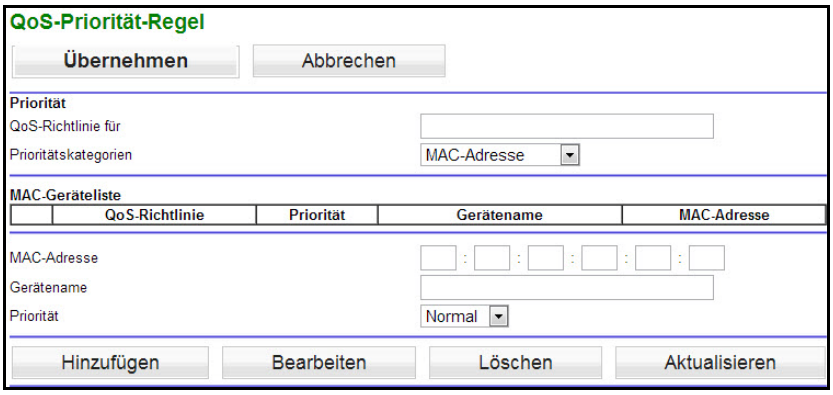
➢ **So erstellen Sie eine QoS-Richtlinie für ein Gerät, das an einen der LAN-Ports des Modemrouters angeschlossen ist:**

1. Wählen Sie **QoS Setup** (QoS Konfigurieren) aus, um den Bildschirm **QoS Setup** (QoS Konfigurieren) anzuzeigen. Aktivieren Sie das Kontrollkästchen **Turn Internet Access QoS On** (QoS für Internetzugang aktivieren).
2. Klicken Sie auf die Schaltfläche **Setup QoS Rule** (QoS-Regel festlegen).
3. Klicken Sie auf die Schaltfläche **Add Priority Rule** (Prioritätsregel hinzufügen).
4. Wählen Sie aus der Liste **Priority Category** (Prioritätskategorien) die Option **Ethernet LAN Port** (Netzwerk-LAN-Port) aus.
5. Wählen Sie aus der Liste **LAN Port** (LAN-Port) den LAN-Port aus.
6. Wählen Sie aus der Liste **Priority** (Priorität) die Priorität aus, die dem Datenverkehr dieses Ports beim Internetzugriff im Vergleich zu anderen Anwendungen zugeordnet werden soll. Die verfügbaren Optionen sind **Low** (Niedrig), **Normal**, **High** (Hoch) und **Highest** (Höchste).
7. Klicken Sie auf **Apply** (Übernehmen), um diese Regel in der Liste der QoS-Richtlinien zu speichern, und kehren Sie zum Bildschirm **QoS Setup** (QoS Konfigurieren) zurück.
8. Klicken Sie im Bildschirm **QoS Setup** (QoS Konfigurieren) auf **Apply** (Übernehmen).

QoS für eine MAC-Adresse

➢ **So erstellen Sie eine QoS-Richtlinie für Datenverkehr von einer bestimmten MAC-Adresse:**

1. Wählen Sie **QoS Setup** (QoS Konfigurieren) aus, und klicken Sie auf die Schaltfläche **Setup QoS Rule** (QoS-Regel festlegen). Der Bildschirm **QoS Setup** (QoS Konfigurieren) wird geöffnet.
2. Klicken Sie auf **Add Priority Rule** (Prioritätsregel hinzufügen).
3. Wählen Sie aus der Liste **Priority Category** (Prioritätskategorien) die Option **MAC Address** (MAC-Adresse) aus:



4. Aktivieren Sie die Optionsschaltfläche des Geräts, falls es sich in der Liste der MAC-Geräte befindet. Der Richtlinienname, die MAC-Adresse und der Gerätename werden mit den Informationen aus der Liste der MAC-Geräte ausgefüllt. Klicken Sie auf **Refresh** (Aktualisieren), wenn sich das Gerät nicht in der Liste befindet. Falls es auch dann nicht angezeigt wird, müssen Sie diese Felder manuell ausfüllen.
5. Wählen Sie aus der Liste **Priority** (Priorität) die Priorität aus, die dem Datenverkehr dieses Geräts beim Internetzugriff im Vergleich zu anderen Anwendungen und Datenverkehrstypen zugeordnet werden soll. Die verfügbaren Optionen sind **Low** (Niedrig), **Normal**, **High** (Hoch) und **Highest** (Höchste).
6. Klicken Sie auf **Apply** (Übernehmen), um diese Regel in der Liste der QoS-Richtlinien zu speichern, und kehren Sie zum Bildschirm **QoS Setup** (QoS Konfigurieren) zurück.
7. Aktivieren Sie auf dem Bildschirm **QoS Setup** (QoS Konfigurieren) das Kontrollkästchen **Turn Internet Access QoS On** (QoS für Internetzugang aktivieren).
8. Klicken Sie auf **Apply** (Übernehmen).

Bearbeiten oder Löschen einer vorhandenen QoS-Richtlinie

➢ **So bearbeiten oder löschen Sie eine QoS-Richtlinie:**

1. Wählen Sie **QoS Setup** (QoS Konfigurieren) aus, um den Bildschirm **QoS Setup** (QoS Konfigurieren) anzuzeigen.
2. Aktivieren Sie die Optionsschaltfläche neben der QoS-Richtlinie, die Sie bearbeiten oder löschen möchten, und führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Löschen** (Delete), um die QoS-Richtlinie zu entfernen.
   - Klicken Sie auf **Edit** (Bearbeiten), um die QoS-Richtlinie zu bearbeiten. Befolgen Sie die Anweisungen in den vorhergehenden Abschnitten, um die Richtlinieneinstellungen zu ändern.
3. Klicken Sie auf dem Bildschirm **QoS Setup** (QoS Konfigurieren) auf **Apply** (Übernehmen), um die Änderungen zu speichern.

Sicherheitseinstellungen

4

Informationen auf der Registerkarte **Security** (Sicherheit)

Sie können viele Firewall-Einstellungen nach Ihren Erfordernissen anpassen. Dieses Kapitel enthält die folgenden Abschnitte:

- *Regeln für die Firewall zur Steuerung des Netzwerkzugangs*
- *Webseiten sperren*
- *Regeln für die Firewall zur Steuerung des Netzwerkzugangs*
- *Zeitzone einstellen*
- *Zeitplan für Dienstsperren*
- *Konfigurieren von E-Mail-Warnmeldungen*
- *Portweiterleitung und Port-Triggering*
- *Konfigurieren der Portweiterleitung an lokale Server*
- *Konfigurieren des Port-Triggering*

Regeln für die Firewall zur Steuerung des Netzwerkzugangs

Ihr Modemrouter verfügt über eine Firewall, die unbefugte Zugriffe auf Ihr WLAN-Netzwerk blockiert und autorisierte eingehende und ausgehende Kommunikation erlaubt. Autorisierte Kommunikation wird anhand von Regeln für eingehenden und ausgehenden Datenverkehr konfiguriert. Die Firewall bietet die folgenden zwei Standardregeln. Sie können benutzerdefinierte Regeln erstellen, um die ausgehende Kommunikation weiter einzuschränken oder die eingehende Kommunikation weiter zu öffnen:

- **Inbound** (Eingehend): Alle Zugriffe von außen sperren, außer Antworten auf Anfragen aus dem LAN.
- **Outbound** (Ausgehend): Alle Zugriffe aus dem LAN nach außen zulassen.

Eingangsregeln (Portweiterleitung)

Da der Modemrouter NAT (Network Address Translation) verwendet, wird Ihr Netzwerk vom Internet als eine einzige IP-Adresse erkannt. Benutzer von außerhalb können nicht direkt auf einen Ihrer lokalen Computer zugreifen. Durch die Definition einer Eingangsregel können Sie jedoch einen lokalen Server (z. B. einen Webserver oder Spieleserver) im Internet sichtbar und verfügbar machen.

Die Regel sorgt dafür, dass der Modemrouter eingehenden Datenverkehr für einen bestimmten Dienst auf Grundlage der Portnummer des Ziels an einen lokalen Server weiterleitet. Dieser Vorgang ist auch unter dem Namen Portweiterleitung bekannt. Das Zulassen eingehender Dienste führt zu Öffnungen in der Firewall. Aktivieren Sie nur die Ports, die für das Netzwerk erforderlich sind. Im Folgenden werden zwei Beispiele für Eingangsregeln erläutert.

Hinweis: Einige wohnsitzabhängige Breitband-ISP-Konten lassen die Ausführung von Serverprozessen (z. B. Web- oder FTP-Server) von Ihrem Standort nicht zu. Möglicherweise überprüft Ihr ISP regelmäßig, ob Server betrieben werden, und setzt Ihr Konto aus, wenn aktive Dienste an Ihrem Standort erkannt werden. Wenn Sie nicht sicher sind, lesen Sie die Richtlinien Ihres ISPs zur zulässigen Nutzung.

Ausgangsregeln (Dienstsperren)

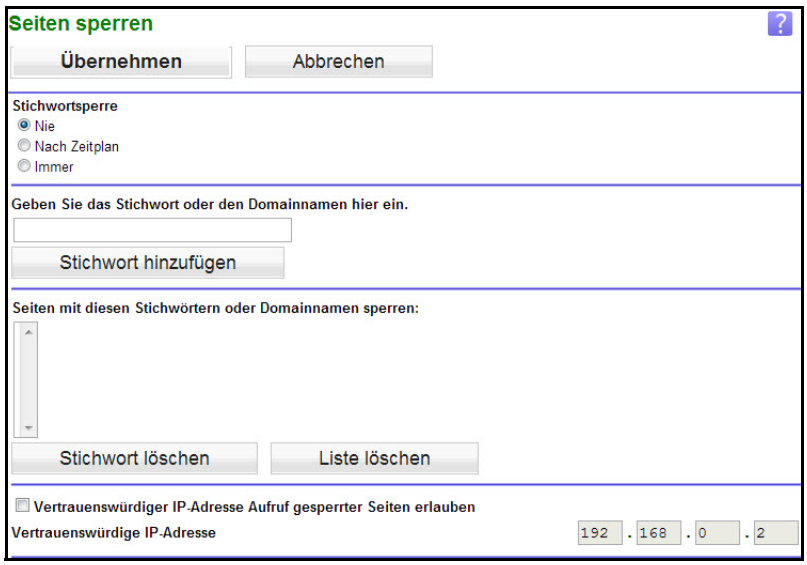
Sie können Computer in Ihrem lokalen Netzwerk blockieren, sodass bestimmte Internetdienste nicht verwendet werden können. Diese Funktion wird als Dienstsperre oder Portfilterung bezeichnet. Sie können eine Ausgangsregel hinzufügen, um Internetzugriff von einem lokalen Computer basierend auf dem Computer, der Internetwebsite, der Tageszeit und dem Diensttyp zu blockieren.

Webseiten sperren

Mit der Stichwortsperre können Sie verhindern, dass bestimmte Arten von HTTP-Datenverkehr auf das Netzwerk zugreifen können. Die Sperre kann permanent oder nach einem Zeitplan eingerichtet werden.

➢ **So blockieren Sie den Datenverkehr:**

1. Wählen Sie **Security** (Sicherheit) **> Block Sites** (Seiten sperren).



2. Wählen Sie eine der Optionen für die Stichwortsperre aus:
   - **Per Schedule** (Nach Zeitplan): Aktiviert die Stichwortsperre unter Berücksichtigung der Einstellungen auf dem Bildschirm **Schedule** (Zeitplan)
   - **Always** (Immer): Aktiviert die permanente Stichwortsperre unabhängig von den Einstellungen auf dem Bildschirm **Schedule** (Zeitplan)
3. Geben Sie ein Stichwort oder eine Domain in das Stichwortfeld ein, klicken Sie auf **Add Keyword** (Stichwort hinzufügen), und klicken Sie auf **Apply** (Übernehmen).

   Es werden bis zu 32 Einträge in der Stichwortliste unterstützt. Hier finden Sie einige Beispiele:

   - Geben Sie **XXX** an, um **http://www.badstuff.com/xxx.html** zu sperren.
   - Geben Sie **.com** an, um nur Internetseiten mit anderen Domainerweiterungen, wie **.edu** oder **.gov**, zuzulassen.
   - Geben Sie einen Punkt (**.**) ein, um den gesamten Zugriff auf das Internet zu sperren.

➢ **So löschen Sie Stichwörter:**

1. Wählen Sie das Stichwort oder die Domain, das/die Sie von der Liste entfernen wollen.
2. Klicken Sie auf **Delete Keyword** (Stichwort löschen) und danach auf **Apply** (Übernehmen), um die Änderungen zu speichern.

Sie können einen vertrauenswürdigen Computer von der Sperre und Protokollierung ausnehmen. Der ausgenommene Computer muss über eine statische IP-Adresse verfügen.

➢ **So geben Sie einen vertrauenswürdigen Computer an:**

1. Geben Sie die IP-Adresse in das Feld **Trusted IP Address** (Vertrauenswürdige IP-Adresse) ein.
2. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

Regeln für die Firewall zur Steuerung des Netzwerkzugangs

Die Firewall bietet folgende Standardregeln:

- **Inbound** (Eingehend): Alle Zugriffe von außen sperren, außer Antworten auf Anfragen aus dem LAN.
- **Outbound** (Ausgehend): Alle Zugriffe aus dem LAN nach außen zulassen.

Regeln für die Firewall konfigurieren

Sie können benutzerdefinierte Regeln erstellen, um die ausgehende Kommunikation weiter einzuschränken oder die eingehende Kommunikation weiter zu öffnen. Über den Bildschirm **Firewall Rules** (Regeln für die Firewall) können Sie benutzerdefinierte Regeln hinzufügen, um Ausnahmen zu den Standardregeln zu definieren. Ausnahmen können anhand des Dienstes oder der IP-Adresse der Anwendung, der Quelle oder des Ziels sowie der Tageszeit eingerichtet werden. Sie können den Datenverkehr protokollieren, auf den die Regel zutrifft oder nicht zutrifft und die Reihenfolge der Prioritäten der Regeln ändern.

Alle Daten, die versuchen, durch die Firewall zu gelangen, werden den Regeln in der in der Regeltabelle angezeigten Reihenfolge unterworfen: von oben (höchste Priorität) nach unten zu den Standardregeln. In manchen Fällen ist die Reihenfolge der Prioritäten wichtig, um festzustellen, welche eingehende oder ausgehende Kommunikation zulässig ist.

➢ **So richten Sie Regeln für die Firewall ein:**

1. Klicken Sie auf **Security > Firewall Rules** (Sicherheit > Regeln für die Firewall).

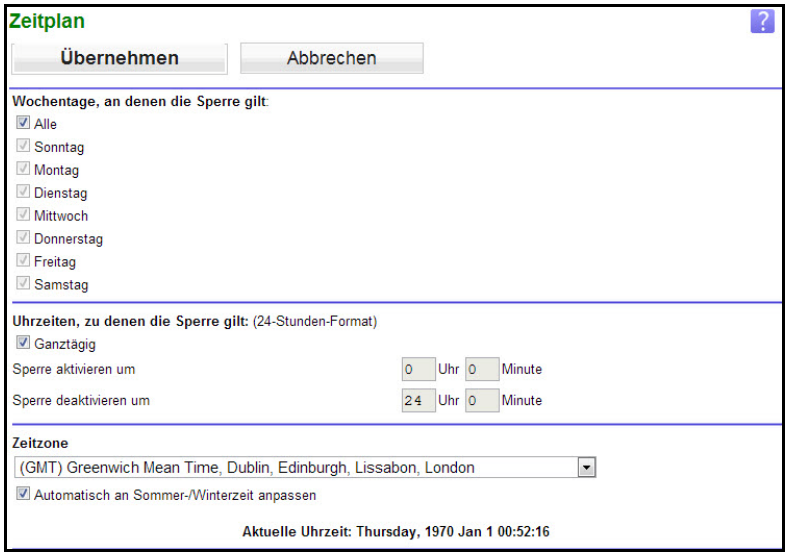
2. Zum Hinzufügen einer Ausgangsregel klicken Sie auf **Add** (Hinzufügen) unter **Outbound Services** (Ausgehende Dienste). Zum Ändern oder Löschen einer Regel wählen Sie die entsprechende Schaltfläche auf der linken Seite und klicken auf **Edit** (Bearbeiten) oder **Delete** (Löschen).
3. So ändern Sie die Reihenfolge der Prioritäten:
   a. Wählen Sie die Schaltfläche auf der linken Seite der Regel, und klicken Sie auf **Move** (Verschieben).
   b. Geben Sie die Nummer der neuen Position ein, und klicken Sie auf **OK**.
4. Zum Öffnen oder Schließen von Instant Messaging aktivieren Sie eine der folgenden Optionsschaltflächen:
   - **Close IM Ports** (IM-Ports schließen): Deaktiviert den Instant-Messaging-Datenverkehr.
   - **Open IM Ports** (IM-Ports öffnen): Aktiviert den Instant-Messaging-Datenverkehr. IM-Ports sind standardmäßig offen.
5. Klicken Sie auf **Apply** (Übernehmen): um die Einstellungen zu speichern.

Zeitzone einstellen

Der Modemrouter nutzt das NTP-Protokoll (Network Time Protocol) zum Abruf der aktuellen Uhrzeit und des Datums von einem der NTP-Server im Internet.

➢ **So stellen Sie die Zeitzone ein:**

1. Wählen Sie **Security** (Sicherheit) > **Schedule** (Zeitplan).



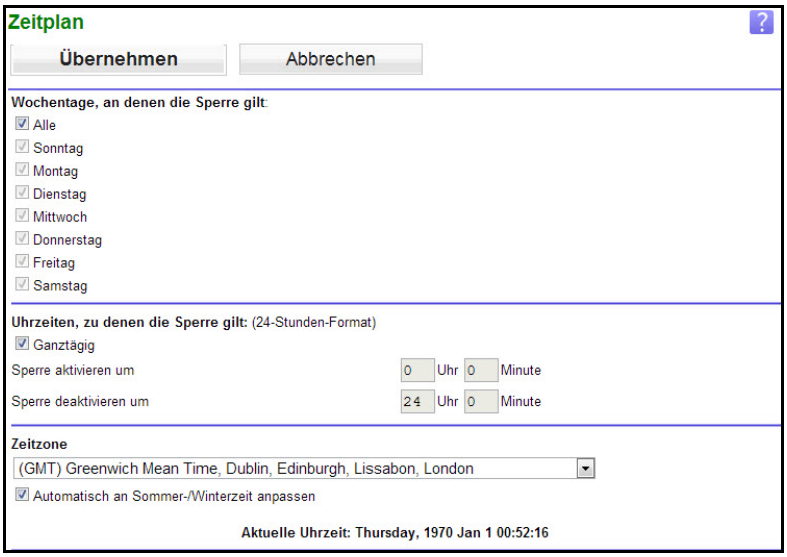
2. Wählen Sie Ihre Zeitzone aus. Diese Einstellung legt den Zeitplans für Sperren und die zeitliche Bestimmung von Protokolleinträgen fest.
3. Wenn während der Sommermonate auf Sommerzeit umgestellt wird, aktivieren Sie das Kontrollkästchen **Automatically adjust for daylight savings time** (Automatisch an Sommer-/Winterzeit anpassen).
4. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Zeitplan für Dienstsperren

Wenn Sie Dienstsperren im Bildschirm **Block Services** (Dienste sperren) bzw. Port-Forwarding im Bildschirm **Ports** aktiviert haben, können Sie in einem Zeitplan festlegen, wann die Sperrung erfolgen soll bzw. wann der Zugriff nicht eingeschränkt wird.

➢ **So richten Sie einen Zeitplan für Dienste ein:**

1. Wählen Sie **Security** (Sicherheit) > **Schedule** (Zeitplan).



2. Zur Sperrung von Internetdiensten anhand eines Zeitplans wählen Sie **Every Day** (Alle) oder einen oder mehrere Tage.
3. Wenn die Zugriffsbeschränkungen an den gewählten Wochentagen rund um die Uhr gelten sollen, wählen Sie **All Day** (Ganztätig). Andernfalls geben Sie die Zeitpunkte in die Felder **Start Blocking** (Sperre aktivieren um) und **End Blocking** (Sperre deaktivieren um) ein.

   Hinweis: *Geben Sie die Werte im 24-Stunden-Format ein. Beispiel: 10:30 bedeutet 10 Uhr und 30 Minuten morgens, und 22:30 bedeutet 10 Uhr und 30 Minuten abends. Wenn Sie die Startzeit nach der Endzeit ansetzen, gilt der Zeitplan über den Tageswechsel hinaus.*

4. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Konfigurieren von E-Mail-Warnmeldungen

Wenn Sie Protokolle und Warnungen per E-Mail erhalten möchten, geben Sie Ihre E-Mail-Informationen auf dem Bildschirm **E-mail** (E-Mail) ein, und geben Sie an, welche Warnungen Sie mit welcher Regelmäßigkeit erhalten möchten.

Wählen Sie **Security** (Sicherheit) > **Email** (E-Mail). Der folgende Bildschirm wird angezeigt:

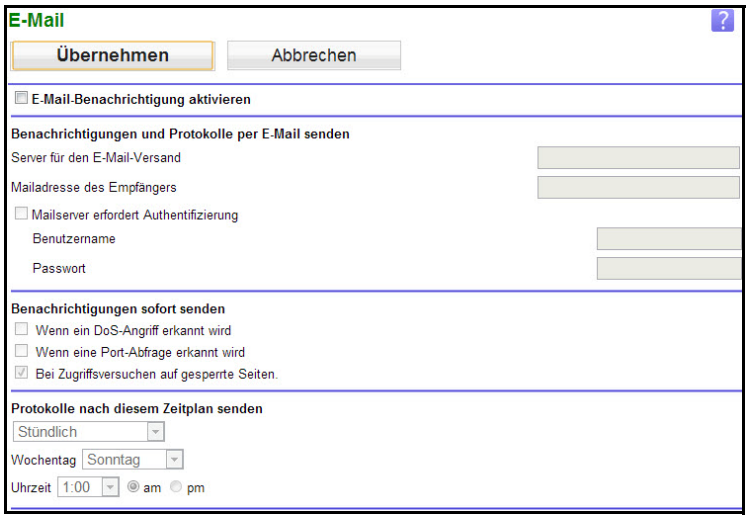


Abbildung 8. Bildschirm E-Mail

- **Turn E-mail Notification On** (E-Mail-Benachrichtigung aktivieren): Aktivieren Sie dieses Kontrollkästchen, wenn Sie vom Modemrouter Protokolle und Benachrichtigungen per E-Mail erhalten möchten.
- **Send to This E-mail Address** (Mailadresse des Empfängers): Geben Sie die E-Mail-Adresse ein, an die Protokolle und Benachrichtigungen gesendet werden sollen. Diese E-Mail-Adresse wird auch als Absender angegeben. Wenn Sie dieses Feld leer lassen, werden keine Protokolle und Warnmeldungen per E-Mail gesendet.
- **Your Outgoing Mail Server** (Server für den E-Mail-Versand): Geben Sie den Namen oder die IP-Adresse des SMTP-Servers Ihres ISP (für abgehende E-Mail-Nachrichten) ein (z. B. mail.meinISP.de). Möglicherweise finden Sie diese Informationen in den Konfigurationseinstellungen Ihres E-Mail-Programms. Geben Sie die E-Mail-Adresse ein, an die Protokolle und Benachrichtigungen gesendet werden sollen. Diese E-Mail-Adresse wird auch als Absender angegeben. Wenn Sie dieses Feld leer lassen, werden keine Protokolle und Warnmeldungen per E-Mail gesendet.
- **My mail server requires authentication** (Mailserver erfordert Authentifizierung): Wenn Sie einen Postausgangsserver verwenden, der von Ihrem gegenwärtigen ISP bereitgestellt wird, müssen Sie dieses Feld nicht aktivieren. Wenn Sie ein E-Mail-Konto verwenden, das nicht von Ihrem ISP bereitgestellt wird, aktivieren Sie dieses Feld, und geben Sie die erforderlichen Zugangsdaten (Benutzername und Passwort) an.
- **Send Alerts Immediately** (Benachrichtigungen sofort senden): Aktivieren Sie das entsprechende Kontrollkästchen, wenn Sie sofortige Benachrichtigungen über wichtige sicherheitsrelevante Ereignisse wünschen, beispielsweise einen erkannten Angriff, einen Port-Scan oder den versuchten Zugriff auf eine gesperrte Seite.

- **Send logs according to this schedule** (Protokolle nach diesem Zeitplan senden): Damit geben Sie an, wie oft die Protokolle gesendet werden sollen: Keine, Stündlich, Täglich, Wöchentlich oder Bei vollem Protokoll.
  - **Days** (Tage): Gibt an, an welchem Wochentag das Protokoll gesendet werden soll. Dies ist relevant, wenn das Protokoll wöchentlich gesendet wird.
  - **Time** (Uhrzeit): Gibt die Tageszeit an, zu der das Protokoll gesendet werden soll. Dies ist relevant, wenn das Protokoll täglich oder wöchentlich gesendet wird.

Hinweis: Wenn die Option für wöchentliche, tägliche oder stündliche Benachrichtigung gewählt wurde und das Protokoll vor Ablauf der angegebenen Zeit voll ist, wird es automatisch an die angegebene E-Mail-Adresse gesendet. Nach dem Senden des Protokolls wird dieses automatisch aus dem Speicher des Modemrouters gelöscht. Wenn der Modemrouter die Protokolldatei nicht per E-Mail senden kann, wird der Protokoll-Zwischenspeicher möglicherweise zu voll. In diesem Fall überschreibt der Modemrouter das Protokoll und löscht seinen Inhalt.

Portweiterleitung und Port-Triggering

Standardmäßig blockiert der Modemrouter eingehenden Datenverkehr aus dem Internet auf Ihre Computer, mit Ausnahme von Antworten auf abgehenden Datenverkehr. Möglicherweise müssen Sie Ausnahmen für diese Regel festlegen, z. B. in den folgenden Fällen:

- Remote-Computer im Internet müssen auf einen Server im lokalen Netzwerk zugreifen.
- Bestimmte Anwendungen und Spiele können andernfalls nicht ordnungsgemäß ausgeführt werden, da ihre Antworten vom Router nicht immer erkannt werden.

Der Modemrouter bietet zwei Funktionen für die Erstellung dieser Ausnahmen: Portweiterleitung und Port-Triggering. Die folgenden Abschnitte enthalten Hintergrundinformationen zu diesem Thema, um die Funktion von Portweiterleitung und Port-Triggering zu erläutern und die Unterschiede zwischen diesen beiden Konzepten aufzuzeigen.

Grundlegende Informationen zum Remote-Computerzugriff

Wenn ein Computer im Netzwerk auf einen Computer im Internet zugreifen muss, sendet der Computer Ihrem Modemrouter eine Meldung mit der Quell- und Zieladresse und den Prozessinformationen. Vor der Weiterleitung der Meldung an den Remote-Computer muss der Modemrouter die Quellinformationen ändern und die Sitzung für den Datenaustausch erstellen und nachverfolgen, damit Antworten zurück auf den Computer geleitet werden können.

Es folgt ein Beispiel für normalen abgehenden Datenverkehr und die darauf folgenden eingehenden Antworten:

1. Sie öffnen einen Browser, und Ihr Betriebssystem weist dieser Browsersitzung die Portnummer 5678 zu.
2. Sie geben in das URL-Feld die Adresse http://www.beispiel.de ein, und Ihr Computer erstellt eine Meldung für die Anforderung einer Webseite mit den folgenden Adress- und Portinformationen. Die Anforderung wird an den Modemrouter gesendet.

   Quelladresse: Die IP-Adresse des Computers

   Quellportnummer: 5678, die Portnummer der Browsersitzung

   Zieladresse: Die IP-Adresse der URL **www.beispiel.de**, die Ihr Computer durch eine Anfrage beim DNS-Server ermittelt

   Zielportnummer: 80, die Standardportnummer eines Webserver-Prozesses
3. Der Modemrouter erstellt einen Eintrag in der Tabelle für interne Sitzungen und beschreibt diese Sitzung für den Datenaustausch zwischen Ihrem Computer und dem Webserver unter www.beispiel.de. Bevor die Anforderung der Webseite an www.beispiel.de gesendet wird, speichert der Modemrouter die ursprünglichen Informationen und ändert dann die Quellinformationen der Anforderung, d. h., er führt eine Network Address Translation (NAT) durch:
   - Die Quelladresse wird durch die öffentliche IP-Adresse des Modemrouters ersetzt. Dies ist notwendig, da Ihr Computer eine private IP-Adresse verwendet, die nicht weltweit eindeutig ist und im Internet nicht verwendet werden kann.
   - Die Quellportnummer wird zu einer vom Modemrouter zugewiesenen Nummer geändert, z. B. 33333. Dies ist notwendig, da zwei Computer unabhängig voneinander dieselbe Sitzungsnummer verwenden könnten.

   Der Modemrouter sendet daraufhin die Anforderung über das Internet an den Webserver unter **www.beispiel.de**.
4. Der Webserver unter **www.beispiel.de** verfasst eine Rücknachricht mit den angeforderten Webseitendaten. Die Rücknachricht enthält die folgenden Adress- und Portinformationen. Der Webserver sendet diese Antwort danach an den Modemrouter.

   Quelladresse: Die IP-Adresse der URL www.beispiel.de

   Quellportnummer: 80, die Standardportnummer eines Webserver-Prozesses

   Zieladresse: Die öffentliche IP-Adresse des Modemrouters

   Zielportnummer: 33333

5. Nach dem Empfang der eingehenden Nachricht überprüft der Modemrouter über die Sitzungstabelle, ob es eine aktive Sitzung für die Portnummer 33333 gibt. Falls der Modemrouter eine aktive Sitzung findet, ändert er die Nachricht, um die ursprünglichen Adressinformationen wiederherzustellen, die durch den NAT-Vorgang ersetzt wurden. Der Modemrouter sendet die Antwort an den Computer, der die Webseite **www.beispiel.de** anzeigt. Die Nachricht enthält jetzt die folgenden Adress- und Portinformationen.

   Quelladresse: Die IP-Adresse der URL www.beispiel.de

   Quellportnummer: 80, die Standardportnummer eines Webserver-Prozesses

   Zieladresse: Die IP-Adresse des Computers

   Zielportnummer: 5678, die Browsersitzung, von der die erste Anforderung gesendet wurde

6. Nach Beendigung der Browsersitzung entdeckt der Modemrouter möglicherweise einen Zeitraum der Inaktivität in der Kommunikation. Der Modemrouter entfernt daraufhin die Sitzungsinformationen aus der Sitzungstabelle, und eingehender Datenverkehr wird für die Portnummer 33333 nicht mehr akzeptiert.

Port-Triggering zum Öffnen eingehender Ports

Im vorhergehenden Beispiel werden Anforderungen von Ihrem Modemrouter über eine bestimmte Dienstportnummer an einen Remote-Computer gesendet. Die Antworten des Remote-Computers an Ihren Modemrouter werden an diesen Port geleitet. Wenn der Remote-Server eine Antwort zurück an einen anderen Port sendet, akzeptiert der Modemrouter sie nicht und verwirft sie. Einige Anwendungsserver (z. B. FTP- und IRC-Server) senden jedoch Antworten an mehrere Ports zurück. Mit der Funktion **Port-Triggering** des Modemrouters können Sie den Modemrouter so einrichten, dass er zusätzliche eingehende Ports öffnet, wenn ein bestimmter Ausgangs-Port eine Sitzung initiiert.

Ein Beispiel dafür ist IRC (Internet Relay Chat). Ihr Computer stellt eine Verbindung mit einem IRC-Server am Zielport 6667 her. Der IRC-Server antwortet nicht nur über den ursprünglichen Quellport, sondern sendet außerdem eine Identifizierungsnachricht über Port 113 an den Computer. Mit Port-Triggering können Sie dem Modemrouter Folgendes mitteilen: „Wenn eine Sitzung über den Zielport 6667 initiiert wird, muss auch eingehender Datenverkehr über Port 113 den Ursprungscomputer erreichen.“ Mit ähnlichen Schritten wie im vorhergehenden Beispiel sind im Folgenden die Ergebnisse der definierten Port-Triggering-Regel dargestellt:

1. Sie öffnen ein IRC-Clientprogramm, um eine Chatsitzung auf dem Computer zu starten.
2. Der IRC-Client verfasst eine Anforderungsnachricht an einen IRC-Server über die Zielportnummer 6667, die Standardportnummer für einen IRC-Servervorgang. Der Computer sendet diese Antwort danach an den Modemrouter.
3. Der Modemrouter erstellt einen Eintrag in der Tabelle für interne Sitzungen und beschreibt diese Sitzung für den Datenaustausch zwischen Ihrem Computer und dem IRC-Server. Der Modemrouter speichert die ursprünglichen Informationen, führt eine Network Address Translation (NAT) für die Quelladresse und den Quellport aus und sendet diese Anforderung über das Internet an den IRC-Server.

4. Unter Beachtung der Port-Triggering-Regel und mit Berücksichtigung der Zielportnummer 6667 erstellt der Modemrouter einen zusätzlichen Sitzungseintrag, um den für Port 113 eingehenden Datenverkehr an den Computer zu senden.
5. Der IRC-Server sendet eine Rücknachricht über den durch NAT zugewiesenen Quellport (z. B. 33333, wie im vorherigen Beispiel) als Zielport an den Modemrouter. Darüber hinaus sendet der IRC-Server eine Identifizierungsnachricht mit Zielport 113 an den Modemrouter.
6. Nach dem Empfang der eingehenden Nachricht an den Zielport 33333 überprüft der Modemrouter über die Sitzungstabelle, ob es eine aktive Sitzung für die Portnummer 33333 gibt. Nachdem er die aktive Sitzung gefunden hat, stellt der Modemrouter die zuvor über NAT ersetzten ursprünglichen Adressinformationen wieder her und sendet die Rückantwort an den Computer.
7. Nach dem Empfang der eingehenden Nachricht an den Zielport 113 überprüft der Modemrouter die Sitzungstabelle und findet dort eine aktive Sitzung für die Portnummer 113, die Ihrem Computer zugeordnet ist. Der Modemrouter ersetzt die Ziel IP-Adresse der Nachricht durch die IP-Adresse des Computers und leitet die Nachricht an den Computer weiter.
8. Nach Beendigung der Chatsitzung entdeckt der Modemrouter möglicherweise einen Zeitraum der Inaktivität in der Kommunikation. Der Modemrouter entfernt daraufhin die Sitzungsinformationen aus der Sitzungstabelle, und eingehender Datenverkehr wird für die Portnummern 33333 oder 113 nicht mehr akzeptiert.

Damit Sie Port-Triggering konfigurieren können, müssen Sie wissen, welche Eingangs-Ports die Anwendung benötigt. Außerdem müssen Sie die Nummer des Ausgangs-Ports kennen, der die Öffnung der Eingangs-Ports auslöst. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung, Benutzergruppen oder Newsgruppen wenden.

Hinweis: Die Triggering-Anwendung kann immer nur auf einem Computer verwendet werden.

Portweiterleitung zur Zulassung externer Hostkommunikation

In den beiden vorhergehenden Beispielen wurde eine Anwendungssitzung mit einem Server-Computer im Internet von Ihrem Computer initiiert. Möglicherweise müssen Sie jedoch zulassen, dass ein Client-Computer im Internet eine Verbindung zu einem Server-Computer in Ihrem Netzwerk herstellt. Normalerweise ignoriert der Modemrouter eingehenden Datenverkehr, der nicht als Antwort auf Ihren ausgehenden Datenverkehr gesendet wird. Mit der Portweiterleitung können Sie Ausnahmen für diese Standardregel konfigurieren.

Eine häufige Anwendung der Portweiterleitung kann durch die Umkehrung der Client-Server-Beziehung aus dem vorherigen Webserver-Beispiel demonstriert werden. In diesem Fall muss der Browser eines Remote-Computers auf einen Webserver zugreifen, der auf einem Computer im lokalen Netzwerk ausgeführt wird. Mit der Portweiterleitung können Sie dem Modemrouter Router Folgendes mitteilen: „Wenn eingehender Datenverkehr über Port 80 (Standardportnummer für einen Webserver-Prozess) empfangen wird, muss dieser an den lokalen Computer unter 192.168.0.123 weitergeleitet werden.“ Im Folgenden sind die Ergebnisse der definierten Portweiterleitungsregel dargestellt:

1. Ein Benutzer eines Remote-Computers öffnet einen Browser und fordert eine Webseite von **www.beispiel.de** an, die zur öffentlichen IP-Adresse Ihres Modemrouters aufgelöst wird. Der Remote-Computer erstellt eine Anforderung für eine Webseite mit den folgenden Zielinformationen:

   Zieladresse: Die IP-Adresse von www.beispiel.de, die mit der Adresse des Modemrouters übereinstimmt

   Zielportnummer: 80, die Standardportnummer eines Webserver-Prozesses

   Der Remote-Computer sendet danach diese Anforderung über das Internet an den Modemrouter.

2. Der Modemrouter empfängt die Anforderung und überprüft, ob es in der Regeltabelle eine Regel gibt, die die Art des eingehenden Datenverkehrs an Port 80 abdeckt. In der Portweiterleitungsregel wird angegeben, dass der eingehende Datenverkehr an Port 80 an die lokale IP-Adresse 192.168.0.123 weitergeleitet werden soll. Deshalb ändert der Modemrouter die Zielinformationen in der Anforderung:

   Die Zieladresse wird durch 192.168.0.123 ersetzt.

   Der Modemrouter sendet die Anforderung danach an das lokale Netzwerk.

3. Ihr Webserver unter 192.168.0.123 empfängt die Anforderung und verfasst eine Rücknachricht mit den angeforderten Websitedaten. Der Webserver sendet diese Antwort danach an den Modemrouter.
4. Der Modemrouter führt eine Network Address Translation (NAT) für die Quell-IP-Adresse aus und sendet diese Anforderung über das Internet an den Remote-Computer, der die Webseite von www.beispiel.de anzeigt.

Damit Sie die Portweiterleitung konfigurieren können, müssen Sie wissen, welche Eingangs-Ports die Anwendung benötigt. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung oder die entsprechenden Benutzergruppen und Newsgruppen wenden.

Unterschiede zwischen Portweiterleitung und Port-Triggering

In den folgenden Punkten werden die Unterschiede zwischen Portweiterleitung und Port-Triggering zusammengefasst:

- Port-Triggering kann von jedem beliebigen Computer im Netzwerk verwendet werden, jedoch immer nur von jeweils einem Computer.
- Die Portweiterleitung wird für einen einzelnen Computer im Netzwerk konfiguriert.
- Beim Port-Triggering müssen Sie nicht die IP-Adresse des Computers im Voraus kennen. Die IP-Adresse wird automatisch erfasst.
- Für die Portweiterleitung müssen Sie die IP-Adresse des Computers während der Konfiguration angeben, und die IP-Adresse darf sich nicht ändern.
- Für das Port-Triggering müssen durch bestimmten abgehenden Datenverkehr Eingangs-Ports geöffnet werden. Die Triggering-Ports werden nach einem bestimmten Zeitraum der Inaktivität geschlossen.
- Die Portweiterleitung ist immer aktiv und muss nicht durch Triggering ausgelöst werden.

Konfigurieren der Portweiterleitung an lokale Server

Mit der Portweiterleitung können Sie zulassen, dass bestimmte eingehende Datenverkehrstypen Server im lokalen Netzwerk erreichen. Beispiel: Sie möchten einen lokalen Webserver, FTP-Server oder Spieleserver über das Internet sichtbar und verfügbar machen.

Mit dem Bildschirm **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) können Sie den Modemrouter so konfigurieren, dass bestimmte eingehende Protokolle an Computer in Ihrem lokalen Netzwerk weitergeleitet werden. Neben Servern für bestimmte Anwendungen können Sie auch einen DMZ-Standardserver festlegen, an den alle anderen eingehenden Protokolle weitergeleitet werden.

Ermitteln Sie zunächst, welche Art von Dienst, Anwendung oder Spiel Sie bereitstellen möchten. Machen Sie die lokale IP-Adresse des Computers ausfindig, der den Dienst bereitstellen soll. Der Server-Computer muss stets dieselbe IP-Adresse haben.

➢ **So konfigurieren Sie die Portweiterleitung:**

Tipp: Legen Sie über die Adressreservierungsfunktion des Modemrouters fest, dass dem Server-Computer immer dieselbe IP-Adresse zugewiesen wird.

1. Wählen Sie **Advanced Setup** (Erweiterte Einrichtung) > **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) aus. Der folgende Bildschirm wird angezeigt:

   Als Diensttyp wird die Portweiterleitung ausgewählt.

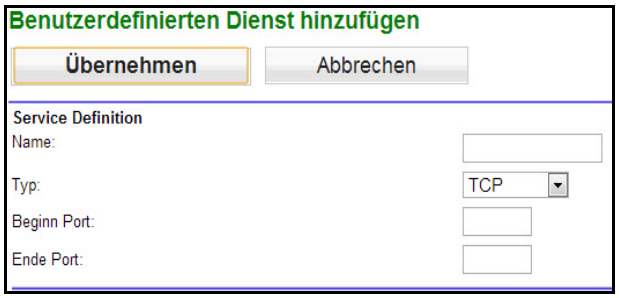
2. Wählen Sie aus der Dropdown-Liste **Service Name** (Dienstname) den Dienst bzw. das Spiel aus, der bzw. das in Ihrem Netzwerk gehostet werden soll. Sollte der Dienst nicht in der Liste angezeigt werden, lesen Sie die Informationen unter *Hinzufügen eines benutzerdefinierten Diensts* auf Seite 61.
3. Klicken Sie auf **Add** (Hinzufügen). Der Dienst wird in der Liste auf dem Bildschirm angezeigt.

Hinzufügen eines benutzerdefinierten Diensts

Zum Definieren von Diensten, Spielen oder Anwendungen, die nicht in der Liste **Service Name** (Dienstname) angezeigt werden, benötigen Sie zuerst die Portnummern oder Portnummernbereiche der Anwendung. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung, Benutzergruppen oder Newsgruppen wenden.

➢ **So fügen Sie einen benutzerdefinierten Dienst hinzu:**

1. Wählen Sie **Advanced** (Erweitert) > **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) aus.
2. Wählen Sie **Port Forwarding** (Portweiterleitung) als Diensttyp aus.
3. Klicken Sie auf die Schaltfläche **Add Custom Service** (Benutzerdefinierten Dienst hinzufügen), um den folgenden Bildschirm anzuzeigen:



4. Geben Sie einen aussagefähigen Namen in das Feld **Name** (Name) ein.
5. Wählen Sie in der Liste das Protokoll aus. Wenn Sie nicht sicher sind, wählen Sie **TCP/UDP** aus.
6. Geben Sie in das Feld **Start Port** (Erster Port) die erste Portnummer ein.
   - Wenn die Anwendung nur einen Port verwendet, geben Sie dieselbe Portnummer in das Feld **End Port** (Letzter Port) ein.
   - Wenn die Anwendung einen Bereich aus mehreren Ports verwendet, geben Sie die Nummer des letzten Ports in diesem Bereich in das Feld **End Port** (Ende Port) ein.
7. Klicken Sie auf **Apply** (Übernehmen). Der Dienst wird in der Liste auf dem Bildschirm **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) angezeigt.

Portweiterleitungseintrag bearbeiten oder löschen

➢ **So bearbeiten oder löschen Sie einen Portweiterleitungseintrag:**

1. Aktivieren Sie in der Tabelle die Optionsschaltfläche neben dem Dienstnamen.
2. Klicken Sie auf **Edit Service** (Dienst bearbeiten) oder **Delete Service** (Dienst löschen).

Anwendungsbeispiel: Veröffentlichen eines lokalen Webservers

Wenn Sie einen Webserver in Ihrem lokalen Netzwerk hosten, können Sie über die Portweiterleitung festlegen, dass Webanforderungen von anderen Personen im Internet Ihren Webserver erreichen.

➢ **So veröffentlichen Sie einen lokalen Webserver:**

1. Weisen Sie dem Webserver entweder eine feste IP-Adresse oder eine dynamische IP-Adresse mit DHCP-Adressreservierung zu. In diesem Beispiel vergibt der Modemrouter stets die IP-Adresse 192.168.0.33 an den Webserver.
2. Konfigurieren Sie den Modemrouter im Bildschirm **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) so, dass der HTTP-Dienst an die lokale Adresse Ihres Webservers unter 192.168.0.33 weitergeleitet wird.Modemrouter HTTP (Port 80) ist das Standardprotokoll für Webserver.
3. (Optional) Registrieren Sie einen Hostnamen bei einem dynamischen DNS-Dienst, und konfigurieren Sie den Modemrouter für die Verwendung des Namens, wie unter *Dynamisches DNS* auf Seite 82 beschrieben. Damit ein Remote-Benutzer über das Internet auf Ihren Webserver zugreifen kann, muss er die IP-Adresse kennen, die Ihnen von Ihrem ISP zugewiesen wurde. Falls Sie einen dynamischen DNS-Dienst verwenden, kann der Remote-Benutzer Ihren Server jedoch über einen benutzerfreundlichen Internetnamen erreichen, z. B. **meinnetzwerk.dyndns.org**.

Konfigurieren des Port-Triggering

Port-Triggering ist eine dynamische Erweiterung der Portweiterleitung, die in den folgenden Fällen hilfreich sein kann:

- Mehr als ein lokaler Computer benötigt die Port-Weiterleitung für dieselbe Anwendung (jedoch nicht gleichzeitig).
- Eine Anwendung muss Eingangs-Ports öffnen, die sich vom Ausgangs-Port unterscheiden.

Bei Aktivierung des Port-Triggering überwacht der Modemrouter abgehenden Datenverkehr und sucht nach einem angegebenen abgehenden Trigger-Port. Wenn der Modemrouter abgehenden Datenverkehr an diesem Port registriert, speichert er die IP-Adresse des lokalen Computers, der die Daten gesendet hat. Der Modemrouter öffnet daraufhin vorübergehend den angegebenen Eingangs-Port bzw. die Eingangs-Ports und leitet eingehenden Datenverkehr für die Triggering-Ports an den Triggering-Computer weiter.

Bei der Portweiterleitung wird eine statische Zuordnung einer Portnummer oder eines Portbereichs für einen einzelnen lokalen Computer erstellt. Beim Port-Triggering können Ports für einen beliebigen Computer, der diese erfordert, geöffnet und wieder geschlossen werden, nachdem der Zugang nicht mehr benötigt wird.

Hinweis: Wenn Sie Anwendungen wie Multi-Player-Games, Peer-to-Peer-Verbindungen und Echtzeitkommunikation (z. B. Instant Messaging oder die Remoteunterstützung von Windows XP) verwenden, sollten Sie auch UPnP (Universal Plug and Play) aktivieren. Befolgen Sie dazu die Anweisungen unter *Universal Plug and Play* auf Seite 86.

Damit Sie Port-Triggering einrichten können, müssen Sie wissen, welche Eingangs-Ports die Anwendung benötigt, und Sie müssen die Nummer des Ausgangs-Ports kennen, der die Öffnung der Eingangs-Ports auslöst. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung, Benutzergruppen oder Newsgruppen wenden.

➢ **So konfigurieren Sie Port-Triggering:**

1. Wählen Sie **Advanced** (Erweitert) > **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) aus.
2. Aktivieren Sie die Optionsschaltfläche **Port Triggering** (Port-Triggering), um die Informationen zum Port-Triggering anzuzeigen.

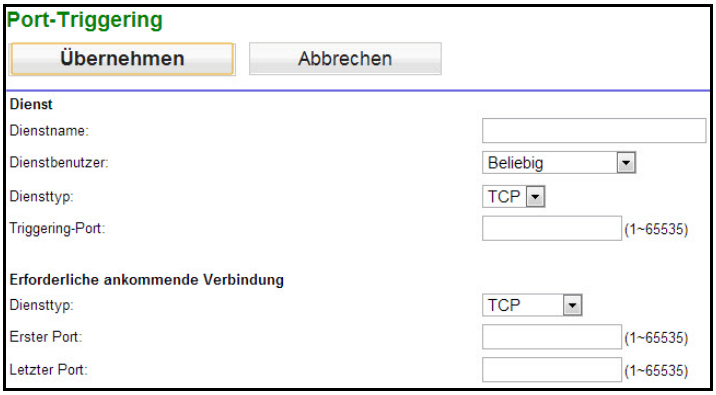
3. Deaktivieren Sie das Kontrollkästchen **Disable Port Triggering** (Port-Triggering deaktivieren), falls es aktiviert ist.

   Hinweis: *Wenn Sie nach der Konfiguration des Port-Triggering das Kontrollkästchen **Disable Port Triggering** (Port-Triggering deaktivieren) aktivieren, wird diese Funktion deaktiviert. Die Port-Triggering-Konfigurationsdaten, die Sie dem Modemrouter hinzugefügt haben, bleiben jedoch erhalten, auch wenn sie nicht verwendet werden.*

4. Geben Sie im Feld **Port Triggering Timeout** (Leerlaufzeit für Port-Triggering) einen Wert von bis zu 9999 Minuten ein.

   Dieser Wert bestimmt, wie lange ein Eingangs-Port geöffnet bleibt, wenn keine weiteren Daten über diesen Port übertragen werden. Die Eingangs-Ports werden geschlossen, wenn der Zeitraum der Inaktivität verstrichen ist. Dies ist erforderlich, da der Modemrouter sonst nicht erkennen kann, wann die Anwendung beendet wurde.

5. Klicken Sie auf **Add Service** (Dienst hinzufügen), um den folgenden Bildschirm anzuzeigen:



6. Geben Sie einen aussagefähigen Dienstnamen in das Feld **Service Name** (Dienstname) ein.
7. Wählen Sie in der Liste **Service User** (Dienstbenutzer) die Standardoption **Any** (Alle) aus, um zuzulassen, dass dieser Dienst von allen Computern im Internet verwendet werden kann. Wählen Sie ansonsten **Single Address** (Einzelne Adresse), und geben Sie die IP-Adresse eines einzelnen Computers ein, wenn nur dieser eine Computer den Dienst nutzen soll.
8. Wählen Sie als Diensttyp **TCP**, **UDP** oder beides (**TCP/UDP**) aus. Wenn Sie nicht sicher sind, wählen Sie **TCP/UDP**.
9. Geben Sie in das Feld **Triggering Port** (Triggering-Port) die Nummer des Ports für den abgehenden Datenverkehr ein, der dafür sorgt, dass die Eingangs-Ports geöffnet werden.
10. Füllen Sie die Portinformationen für die Eingangsverbindung in den Feldern **Connection Type** (Verbindungstyp), **Starting Port** (Erster Port) und **Ending Port** (Letzter Port) aus.
11. Klicken Sie auf **Apply** (Übernehmen). Der Dienst wird in der Zuordnungstabelle für Port-Triggering angezeigt.

Netzwerkverwaltung

5

Optionen auf der Registerkarte **Management** (Verwaltung)

Dieses Kapitel enthält die folgenden Abschnitte:

- *Modemrouter-Firmware aktualisieren*
- *Nach Firmware-Upgrades suchen*
- *Sichern der Einstellungen*
- *Passwort ändern*
- *Routerstatus anzeigen*
- *Angeschlossene Geräte anzeigen*
- *Protokolle*

Modemrouter-Firmware aktualisieren

Die Modemrouter -Firmware (Routing-Software) ist auf einem Flash-Speicher gespeichert. Bei der Anmeldung an Ihrem Modemrouter prüft er standardmäßig die On Networks-Webseite auf neue Firmware und benachrichtigt Sie, falls es eine neuere Version gibt.

WARNUNG:

Achten Sie beim Hochladen der Firmware auf den Modemrouter darauf, dass der Vorgang *nicht* unterbrochen wird (z. B. durch Schließen des Browserfensters, Klicken auf einen Link oder Laden einer neuen Seite). Wenn eine Unterbrechung im Browser stattfindet, wird die Firmware möglicherweise fehlerhaft installiert.

Automatische Firmwareprüfung

Wenn die automatische Firmwareprüfung aktiviert ist, führt der Modemrouter die Prüfung durch und benachrichtigt Sie darüber, ob eine Aktualisierung verfügbar ist oder nicht.

Assistent für die Aktualisierung der Firmware
Abbrechen
Die Verbindung mit dem On Networks-Server wird hergestellt. 1 . Bitte haben Sie etwas Geduld ...

➢ **So prüfen Sie die Firmware automatisch:**

1. Klicken Sie auf **Yes** (Ja), um den Modemrouter zu gestatten, die neue Firmware herunterzuladen und zu installieren Der Aktualisierungsvorgang kann einige Minuten in Anspruch nehmen. Nach dem Hochladen der Firmware wird der Modemrouter neu gestartet.
2. Rufen Sie die N300RM-Supportseite auf, und lesen Sie die Informationen zur neuen Version der Firmware, um herauszufinden, ob Sie den Modemrouter nach der Aktualisierung neu konfigurieren müssen.

Hinweis: Wenn Sie die Meldung **Firmware needs to be reloaded** (Firmware muss neu geladen werden) erhalten, bedeutet dies, dass ein Problem mit der Firmware des Modemrouters festgestellt wurde. Befolgen Sie die Bildschirmanweisungen, um das Problem zu beheben.

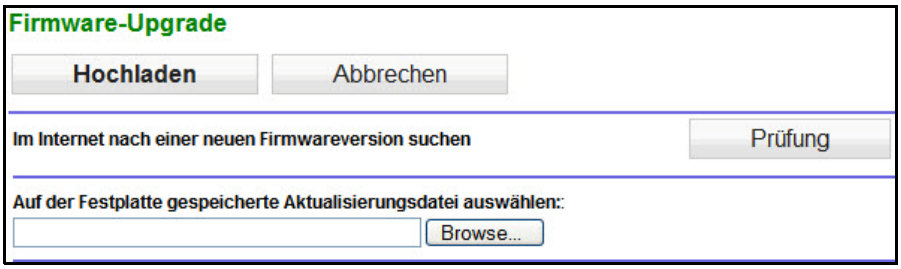
Nach Firmware-Upgrades suchen

Sie können über den Bildschirm **Firmware Upgrade** (Firmware-Upgrade) die On Networks-Webseite nach neueren Versionen der Firmware für Ihr Produkt durchsuchen.

WARNUNG:

Achten Sie beim Hochladen der Firmware auf den Modemrouter darauf, dass der Vorgang *nicht* unterbrochen wird (z. B. durch Schließen des Browserfensters, Klicken auf einen Link oder Laden einer neuen Seite). Wenn eine Unterbrechung im Browser stattfindet, wird die Firmware möglicherweise fehlerhaft installiert.

1. Wählen Sie **Management > Firmware Upgrade** (Verwaltung > Firmware-Upgrade).



2. Klicken Sie auf **Browse** (Durchsuchen), und navigieren Sie zum Firmware-Image, das Sie auf den Computer heruntergeladen haben (die Datei hat die Endung .img oder .chk).
3. Klicken Sie auf **Upload** (Hochladen), um die Firmware auf den Router zu übertragen.

   Nach dem Hochladen der Firmware wird der Modemrouter neu gestartet. Der Aktualisierungsvorgang dauert in der Regel ungefähr eine Minute. Lesen Sie die Versionshinweise der neuen Firmware, um zu überprüfen, ob Sie den Modemrouter nach der Aktualisierung neu konfigurieren müssen.

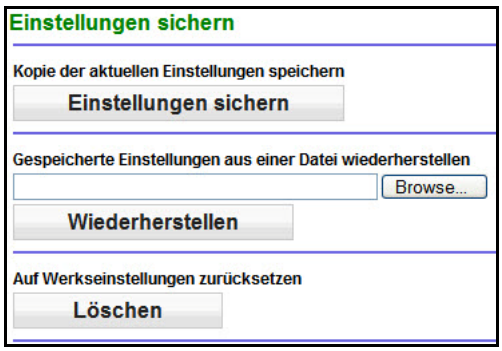
Sichern der Einstellungen

Die Konfigurationseinstellungen des Modemrouters werden in einer Konfigurationsdatei gespeichert (*.cfg). Diese Datei kann auf Ihrem Computer gesichert, wiederhergestellt oder auch zum Zurücksetzen auf die werkseitigen Voreinstellungen verwendet werden.

Sichern

➢ **So sichern Sie die Konfigurationsdatei des Routers:**

1. Wählen Sie **Management** (Verwaltung) > **Backup Settings** (Einstellungen sichern). Der folgende Bildschirm wird angezeigt:



2. Klicken Sie auf **Save** (Speichern), um eine Kopie der aktuellen Einstellungen zu speichern.
3. Wählen Sie einen Speicherort für die Datei mit der Erweiterung **.cfg** auf einem Computer im Netzwerk.

Wiederherstellen

➢ **So stellen Sie die Konfigurationsdatei wieder her:**

1. Geben Sie den vollständigen Netzwerkpfad zur Datei ein, oder klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um die Datei zu suchen.
2. Wenn Sie die Datei mit der Erweiterung **.cfg** gefunden haben, klicken Sie auf die Schaltfläche **Restore** (Wiederherstellen), um die Datei auf den Modemrouter hochzuladen.

   Nach diesem Vorgang wird der Modemrouter neu gestartet.

Löschen

Klicken Sie auf die Schaltfläche **Erase** (Löschen), um den Modemrouter auf die werkseitigen Voreinstellungen zurückzusetzen. Durch Löschen wird das Passwort in **password** und die LAN-IP-Adresse in **192.168.0.1** geändert und das DHCP des Modemrouters aktiviert.

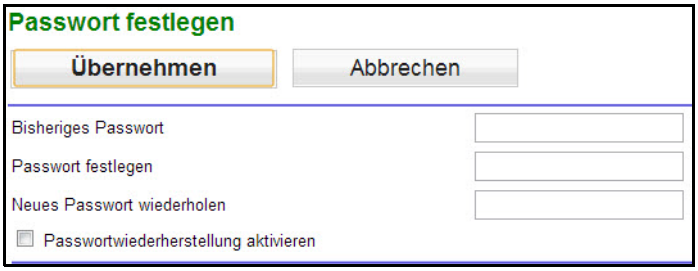
Passwort ändern

Aus Sicherheitsgründen hat der Modemrouter eigene Zugangsdaten (Benutzername und Passwort). Standardmäßig lauten diese **admin** und **password**. Sie können und sollten diese Zugangsdaten ändern und sichere Daten wählen, die Sie sich leicht merken können. Das ideale Passwort enthält keine Wörter aus Wörterbüchern jeglicher Sprache und besteht aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Es kann aus bis zu 30 Zeichen bestehen.

Der Benutzername und das Passwort des Modemrouters unterscheiden sich vom Benutzernamen und Passwort für die Anmeldung zum Herstellen einer Internetverbindung.

➢ **So ändern Sie das Passwort:**

1. Wählen Sie **Management > Set Password** (Verwaltung > Passwort festlegen). Der folgende Bildschirm wird angezeigt:



2. Geben Sie das alte Passwort ein.
3. Geben Sie das neue Passwort zweimal ein.
4. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

Nach Änderung des Passworts müssen Sie sich erneut anmelden, um die Konfiguration fortzuführen. Hinweis: Wenn Sie die Geräteeinstellungen für den Modemrouter gesichert haben, sollten Sie diesen Vorgang nun erneut durchführen, damit das geänderte Passwort in die Sicherungsdatei aufgenommen wird. Informationen zur Sicherung Ihrer Netzwerkkonfiguration finden Sie unter *Sichern* auf Seite 68.

Passwortwiederherstellung

On Networks empfiehlt, die Passwortwiederherstellung zu aktivieren, wenn Sie das Passwort für den Admin-Benutzer des Routers ändern. Wenn Sie das Passwort vergessen, können Sie es wiederherstellen. Die Wiederherstellung wird in Internet Explorer, Firefox und Chrome unterstützt, jedoch nicht in Safari.

➢ **So richten Sie die Passwortwiederherstellung ein:**

1. Aktivieren Sie das Kontrollkästchen **Enable Password Recovery** (Passwortwiederherstellung aktivieren).
2. Wählen Sie zwei Sicherheitsfragen aus, und beantworten Sie sie.
3. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

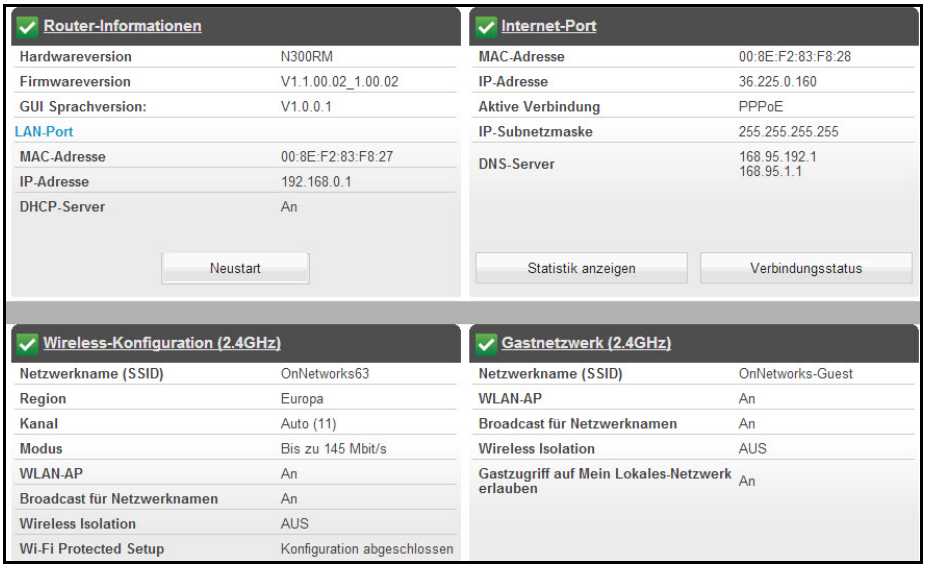
Wenn Sie über den Browser auf den Router zugreifen, wird das Anmeldefenster geöffnet. Bei Aktivierung der Passwortwiederherstellung wird die Passwortwiederherstellung gestartet, nachdem Sie auf **Cancel** (Abbrechen) geklickt haben. Sie können daraufhin die gespeicherten Antworten auf die Sicherheitsfragen eingeben, um das Passwort wiederherzustellen.

Routerstatus anzeigen

Der Bildschirm **Router Status** (Routerstatus) zeigt Status- und Auslastungsinformationen an.

➢ **So zeigen Sie den Routerstatus an:**

Wählen Sie **Management > Router Status** (Verwaltung > Routerstatus). Der folgende Bildschirm wird angezeigt.



Folgende Informationen werden angezeigt:

Router-Informationen

Hardware and Firmware Version (Hardware- und Firmwareversion): Das Hardwaremodell und die aktuell aktive Firmwareversion.

GUI Language Version (GUI Sprachversion): Die aktuell gewählte Sprache.

LAN-Port (Lokale Ports)

MAC Address (MAC-Adresse): Die LAN-Port-MAC-Adresse des Modemrouters.

IP Address (IP-Adresse): Die Modemrouter LAN-Port-IP-Adresse. Die Standardeinstellung ist 192.168.0.1.

DHCP. Ist DHCP ausgeschaltet, so weist der Modemrouter PCs im LAN keine IP-Adressen zu. Ist DHCP eingeschaltet, so weist der Modemrouter Computern im LAN IP-Adressen zu.

Internet-Porteinstellungen

MAC Address (MAC-Adresse): Die MAC-Adresse des DSL-Ports.

IP Address (IP-Adresse): Die IP-Adresse des Internet-Ports. Wenn keine IP-Adresse angezeigt wird, konnte der Modemrouter keine Verbindung zum Internet herstellen.

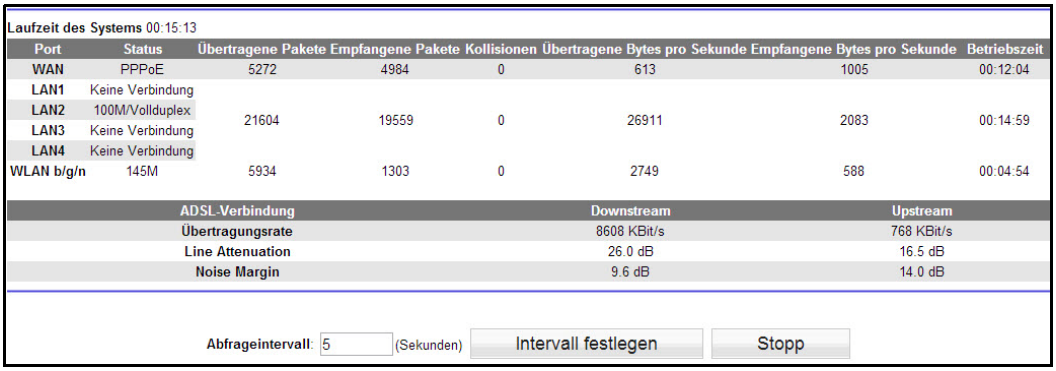
Active Connection (Aktive Verbindung): Der Wert hängt von Ihrem ISP ab.

IP Subnet Mask (IP-Subnetzmaske): Die IP-Subnetzmaske des Internet-Ports.

Domain Name Server (DNS-Server): Die DNS-Server-IP-Adresse des Modemrouters. Diese Adressen werden normalerweise automatisch vom ISP bezogen.

Statistik anzeigen

Klicken Sie auf die Schaltfläche **Show Statistics** (Statistik anzeigen) im Bildschirm **Router Status** (Routerstatus). Ein ähnlicher Bildschirm wie der Folgende wird angezeigt:



Laufzeit des Systems 00:15:13

Port	Status	Übertragene Pakete	Empfangene Pakete	Kollisionen	Übertragene Bytes pro Sekunde	Empfangene Bytes pro Sekunde	Betriebszeit
WAN	PPPoE	5272	4984	0	613	1005	00:12:04
LAN1	Keine Verbindung	21604	19559	0	26911	2083	00:14:59
LAN2	100M/Vollduplex						
LAN3	Keine Verbindung						
LAN4	Keine Verbindung						
WLAN b/g/n	145M	5934	1303	0	2749	588	00:04:54

ADSL-Verbindung	Downstream	Upstream
Übertragungsrate	8608 KBit/s	768 KBit/s
Line Attenuation	26.0 dB	16.5 dB
Noise Margin	9.6 dB	14.0 dB

Abfrageintervall: 5 (Sekunden) Intervall festlegen Stopp

Port

Die Statistiken für die WAN- (Internet), LAN- (lokalen) und WLAN-Ports. Für jeden Port zeigt der Bildschirm Folgendes an:

- **Status**: Der Verbindungsstatus
- **TxPkts** (Übertragene Pakete): Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen übertragen wurden.
- **RxPkts** (Empfangene Pakete): Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen empfangen wurden.
- **Collisions** (Kollisionen): Die Anzahl der Kollisionen seit dem letzten Zurücksetzen oder manuellen Löschen.
- **Tx B/s** (Übertragene Bytes pro Sekunde): Die aktuelle Auslastung der Leitung (in Prozent der momentan genutzten Bandbreite).
- **Rx B/s** (Empfangene Bytes pro Sekunde): Die durchschnittliche Auslastung.
- **Up Time** (Betriebszeit): Die verstrichene Zeit seit dem letzten Neustart oder Zurücksetzen.

ADSL Link Downstream/Upstream (Downstream/Upstream der ADSL-Verbindung)

Die Statistik für den Upstream und Downstream der DSL-Verbindung. Diese Statistik ist für Mitarbeiter des technischen Supports von Interesse, wenn Probleme bei der Herstellung oder Aufrechterhaltung einer Verbindung auftreten.

- **Connection Speed** (Verbindungsgeschwindigkeit): Normalerweise ist die Downstream-Geschwindigkeit höher als die Upstream-Geschwindigkeit.
- **Line Attenuation** (Leitungsdämpfung): Die Leitungsdämpfung erhöht sich, je weiter Sie vom Standort Ihres ISP entfernt sind.
- **Noise Margin** (Störspannungsabstand): Das Verhältnis von Signal zu Störspannung, ein Maß für die Signalqualität der Leitung.
- **Poll Interval** (Abfrageintervall): Zeitabstand, in dem die Statistiken in diesem Fenster aktualisiert werden. Klicken Sie auf die Schaltfläche **Stop** (Stopp), um die Anzeige anzuhalten.

Verbindungsstatus

Klicken Sie im Bildschirm **Router Status** (Routerstatus) auf die Schaltfläche **Connection Status** (Verbindungsstatus):

- **Connection Time** (Verbindungsdauer): Die verstrichene Zeit seit der letzten Verbindung mit dem Internet über den Internet-Port.
- **Connection Status** (Verbindungsstatus): Der Verbindungsstatus.
- **Negotiation** (Verbindungsparameter übermitteln): An oder Aus.
- **Authentication** (Authentifizierung): An oder Aus.
- **IP Address** (IP-Adresse): Die dem WAN-Port durch den ISP zugewiesene IP-Adresse.
- **Subnet Mask** (Subnetzmaske): Die dem WAN-Port durch den ISP zugewiesene Netzwerkmaske.

WLAN-Einstellungen und Gastnetzwerke (2,4GHz)

Unter *WLAN-Konfiguration* auf Seite 32 finden Sie eine ausführliche Beschreibung dieser Einstellungen.

Name (SSID) (Netzwerkname [SSID]): Der Name des WLAN-Netzwerks (Service-Set ID).

Region: Das Land, in dem das Gerät für den Gebrauch eingerichtet ist.

Channel (Kanal): Der aktuelle Kanal, der die Betriebsfrequenz bestimmt.

Mode (Modus): Die aktuelle maximale Datenübertragungsrate in MBit/s.

Wireless AP (WLAN-AP): Zeigt an, ob die Access Point-Funktion aktiviert ist. Wenn diese Funktion nicht aktiviert ist, leuchtet die WLAN-LED vorn am Router nicht.

Broadcast Name (Broadcast für Netzwerknamen): Zeigt an, ob der Modemrouter so konfiguriert ist, dass er seine SSID sendet.

Wireless Isolation: Bei Aktivierung dieser Option können alle WLAN-Computer oder Wireless-Geräte, die mit dem Netzwerk verbunden sind, auf das Internet zugreifen, jedoch nicht auf andere Clients oder Geräte im Netzwerk.

Wi-Fi Protected Setup: Zeigt an, ob das Gerät für WPS in diesem Netzwerk konfiguriert ist.

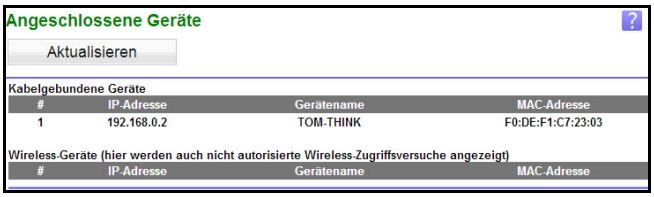
Allow guest to access My Local Network (Gastzugriff auf mein lokales Netzwerk erlauben): Wenn diese Option aktiviert ist, können Nutzer Ihres Gastnetzwerks nicht nur auf Ihr Netzwerk, sondern auch auf die Daten in Ihrem Netzwerk zugreifen.

Angeschlossene Geräte anzeigen

Auf dem Bildschirm **Attached Devices** (Angeschlossene Geräte) werden alle IP-Geräte angezeigt, die der Modemrouter im lokalen Netzwerk erkannt hat.

➢ **So zeigen Sie die angeschlossenen Geräte an:**

Wählen Sie **Management > Attached Devices** (Verwaltung > Angeschlossene Geräte).



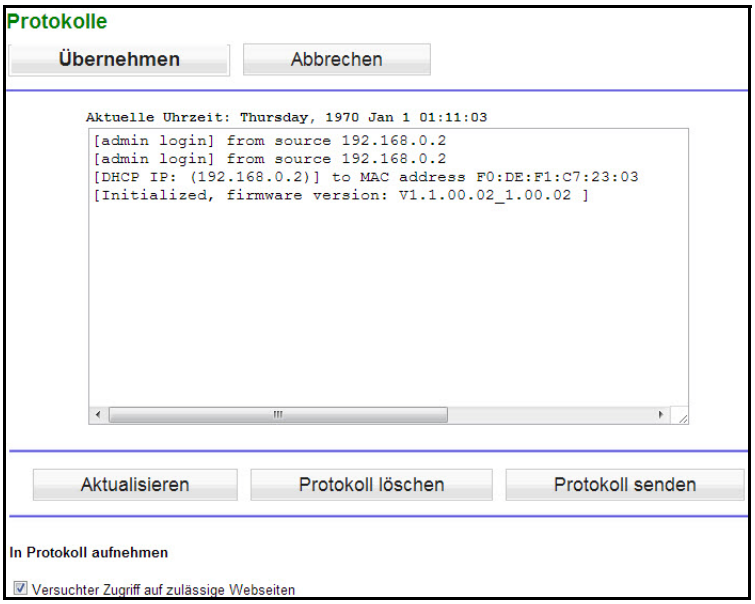
Für jedes Gerät zeigt die Tabelle die IP-Adresse, den Gerätenamen (sofern verfügbar) und die MAC-Adresse. Bei einem Neustart des Modemrouters gehen die Tabellendaten verloren, bis der Modemrouter die Geräte wieder erkennt. Um den Modemrouter zur Suche nach angeschlossenen Geräten zu zwingen, klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).

Protokolle

Der Modemrouter protokolliert sicherheitsrelevante Ereignisse wie abgelehnte eingehende Dienstanforderungen, Erkundungsgänge durch Hacker oder auch Anmeldungen durch den Administrator. Wenn Sie auf dem Bildschirm **Block Sites** (Seiten sperren) einen Contentfilter aktivieren, werden auf dem Bildschirm **Logs** (Protokolle) Zugriffsversuche auf gesperrte Seiten durch Benutzer im Netzwerk angezeigt. Wenn Sie die E-Mail-Benachrichtigung aktivieren, werden diese Protokolle per E-Mail versendet.

➢ **So zeigen Sie das Protokoll an:**

Wählen Sie **Management > Logs** (Verwaltung > Protokolle). Daraufhin erscheint ein Bildschirm wie der folgende:



Mithilfe der Kontrollkästchen **Include in Log** (In Protokoll aufnehmen) können Sie auswählen, welche Ereignisse protokolliert werden sollen. Sie können die Protokolle auf einen Computer schreiben, auf dem ein Syslog-Programm läuft. Zur Aktivierung dieser Funktion wählen Sie **Broadcast on LAN** (Per LAN übertragen) oder geben die IP-Adresse des Servers ein, auf den die Syslog-Datei geschrieben wird. Die Sicherheitsprotokolleinträge enthalten die folgenden Informationen:

- **Date and time** (Datum und Uhrzeit): Datum und Uhrzeit der Aufzeichnung des Protokolleintrags.
- **Description or action** (Beschreibung oder Vorgehensweise): Die Art des Ereignisses und auf welche Weise vorgegangen wurde, falls zutreffend.
- **Source IP** (IP-Quelladresse): Die IP-Adresse des Ausgangsgeräts für diesen Protokolleintrag.
- **Source port and interface** (Quellport und -schnittstelle): Die Portnummer des Dienstes des Ausgangsgeräts und ob es sich im LAN oder im WAN befand.
- **Destination** (Ziel): Der Name oder die IP-Adresse des Zielgeräts oder der Zielwebseite.
- **Destination port and interface** (Zielport und -schnittstelle): Die Portnummer des Dienstes des Zielgeräts und ob es sich im LAN oder im WAN befindet.

Erweiterte Einstellungen

6

Erweiterte Registerkarteneinstellungen für einmalige Situationen

In diesem Kapitel werden die erweiterten Funktionen des Modemrouters beschrieben. Diese Informationen eignen sich für Benutzer mit fortgeschrittenen Netzwerkkenntnissen, die den Modemrouter für einmalige Situationen konfigurieren möchten, etwa wenn Remote-Zugriff über das Internet über IP oder Domainnamen benötigt wird.

> **Hinweis:** Informationen zu Portweiterleitung und Port-Triggering finden Sie unter *Kapitel 4, Sicherheitseinstellungen*.

Dieses Kapitel enthält die folgenden Abschnitte:

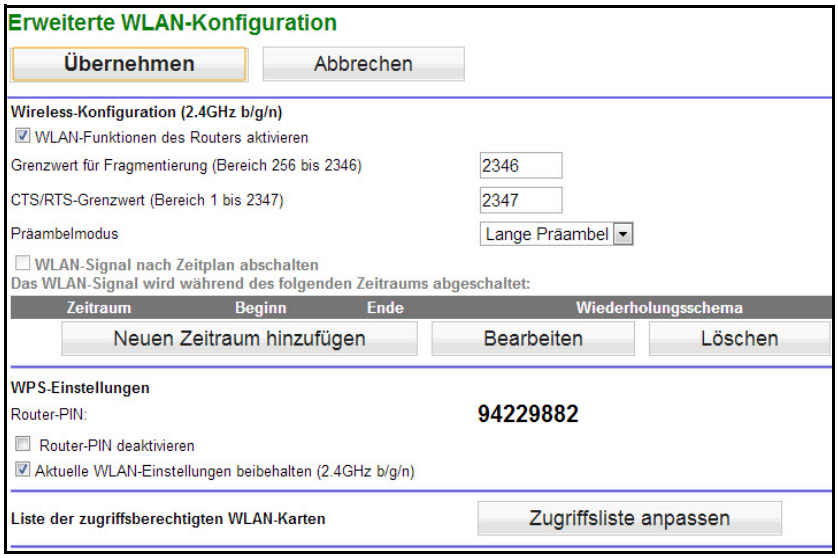
- *Erweiterte WLAN-Konfiguration*
- *WLAN-Repeating (WDS)*
- *Dynamisches DNS*
- *Statische Routen*
- *Fernsteuerung*
- *Universal Plug and Play*
- *Ändern des Gerätemodus*

Erweiterte WLAN-Konfiguration

Standardmäßig wird der Modemrouter mit einer Wireless-Konfiguration eingerichtet, die in den meisten Fällen ausreicht. Auf diesem Bildschirm können Sie die WLAN-Funktionen des Routers steuern und erweiterte Einstellungen auswählen, die für Ihre individuelle Umgebung geeignet sind.

➢ **So zeigen Sie die erweiterte Wireless-Konfiguration an oder ändern diese:**

Wählen Sie **Advanced** (Erweitert) > **Wireless Settings** (Wireless-Konfiguration). Der folgende Bildschirm wird angezeigt:



Dieser Bildschirm enthält die folgenden Einstellungen:

Enable Wireless Router Radio (WLAN-Funktionen des Routers aktivieren): Sie können die WLAN-Funktionen des WLAN-Modemrouters vollständig deaktivieren, indem Sie dieses Kontrollkästchen deaktivieren. Aktivieren Sie das Kontrollkästchen, wenn Sie die WLAN-Funktionen des Modemrouters wieder aktivieren möchten. Wenn das WLAN deaktiviert ist, können andere Mitglieder des Haushalts den Modemrouter verwenden, indem sie ihre Computer mit einem Netzwerkkabel an den Modemrouter anschließen.

Hinweis: Die Optionen **Fragmentation Length** (Fragmentierungsgrenzwert), **CTS/RTS Threshold** (CTS/RTS-Grenzwert) und **Preamble Mode** (Präambelmodus) dienen nur zum Testen des WLAN und der erweiterten Konfiguration. Nehmen Sie keine Änderungen an diesen Einstellungen vor.

Turn off wireless signal by schedule (WLAN-Signal nach Zeitplan abschalten): Mit dieser Funktion können Sie das WLAN-Signal des Modemrouters zu Zeiten, an denen Sie keine WLAN-Verbindung benötigen, abschalten. Beispielsweise können Sie es für das Wochenende deaktivieren, wenn Sie verreisen.

WPS Settings (WPS-Einstellungen): Sie können dem Netzwerk WPS-Geräte hinzufügen.

Wireless Card Access List (Liste der zugriffsberechtigten WLAN-Karten): Klicken Sie auf die Schaltfläche **Set Up Access List** (Zugriffsliste anpassen), um den Bildschirm **Wireless Card Access List** (Liste der zugriffsberechtigten WLAN-Karten) anzuzeigen. Sie können den Netzwerkzugriff auf einzelne Geräte mit vorgegebenen MAC-Adressen beschränken.

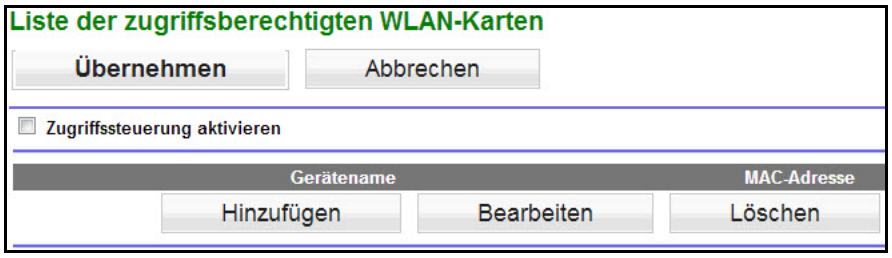
Einschränkung des WLAN-Zugriffs über MAC-Adressen

Sie haben die Möglichkeit, eine Liste der Computer und Wireless-Geräte zu erstellen, die eine Verbindung mit dem WLAN-Netzwerk herstellen können. Grundlage dieser Liste ist die eindeutige MAC-Adresse der Computer und Geräte.

Jedes Netzwerkgerät verfügt über eine MAC-Adresse, die aus einer eindeutigen physischen Adresse aus 12 Zeichen besteht, nur die Hexadezimalzeichen 0-9, a-f oder A-F enthalten kann und Doppelpunkte als Trennzeichen verwendet (z. B. 00:09:AB:CD:EF:01). Normalerweise wird die MAC-Adresse auf dem Etikett der WLAN-Karte oder des Netzabschlussgeräts angegeben. Wenn das Etikett nicht zugänglich ist, können Sie die MAC-Adresse über die Dienstprogramme der Netzwerkkonfiguration des Computers anzeigen. Möglicherweise finden Sie die MAC-Adressen auch im Bildschirm **Attached Devices** (Angeschlossene Geräte).

➢ **So schränken Sie den Zugriff anhand der MAC-Adressen ein:**

1. Klicken Sie auf **Advanced** (Erweitert) **> Wireless Setting** (Wireless-Konfiguration), und wählen Sie **Set Up Access List** (Zugriffsliste anpassen). Der Bildschirm mit der Liste der zugriffsberechtigten WLAN-Karten wird angezeigt.



2. Klicken Sie auf **Add** (Hinzufügen), um ein Wireless-Gerät in die Liste der zugriffsberechtigten WLAN-Karten aufzunehmen.

   Der Bildschirm **Wireless Card Access Setup** (WLAN-Karten einrichten) wird geöffnet. Er enthält eine Liste der aktuell aktiven WLAN-Karten mit den zugehörigen MAC-Adressen.

3. Wenn sich der gewünschte Computer oder das gewünschte Gerät in der Liste **Available Wireless Cards** (Verfügbare WLAN-Karten) befindet, aktivieren Sie die entsprechende Optionsschaltfläche. Geben Sie andernfalls einen Namen und die MAC-Adresse ein. Normalerweise wird die MAC-Adresse auf der Unterseite des Wireless-Geräts angegeben.

   Tipp: Sie können die MAC-Adressen vom Bildschirm **Attached Devices** (Angeschlossene Geräte) des Routers kopieren und in das MAC-Adressfeld dieses Bildschirms einfügen. Stellen Sie dazu von jedem WLAN-Computer eine Verbindung mit dem WLAN-Netzwerk her. Der Computer sollte nun im Bildschirm **Attached Devices** (Angeschlossene Geräte) angezeigt werden.

4. Klicken Sie auf **Add** (Hinzufügen), um dieses Wireless-Gerät in die Liste der zugriffsberechtigten WLAN-Karten aufzunehmen. Der Bildschirm wechselt nun wieder zum Listenbildschirm.
5. Fügen Sie alle Computer oder Geräte hinzu, die eine WLAN-Verbindung herstellen sollen.
6. Aktivieren Sie das Kontrollkästchen **Turn Access Control On** (Zugriffssteuerung aktivieren).
7. Klicken Sie auf **Apply** (Übernehmen).

WLAN-Repeating (WDS)

Sie können den Modemrouter als Wireless Access Point (AP) konfigurieren. Dadurch übernimmt der Modemrouter die Rolle eines WLAN-Repeaters. Ein WLAN-Repeater verbindet sich als Client mit einem anderen WLAN-Modemrouter, wobei das Netzwerk, mit dem die Verbindung besteht, den ISP-Dienst darstellt.

WLAN-Repeating ist eine Art WDS (Wireless Distribution System): Ein WDS ermöglicht es einem WLAN, seine Reichweite über mehrere Access Points zu erweitern, ohne dass zusätzliche Kabel für die Verbindung gelegt werden müssen. In der folgenden Abbildung wird ein WLAN-Repeating-Szenario dargestellt.

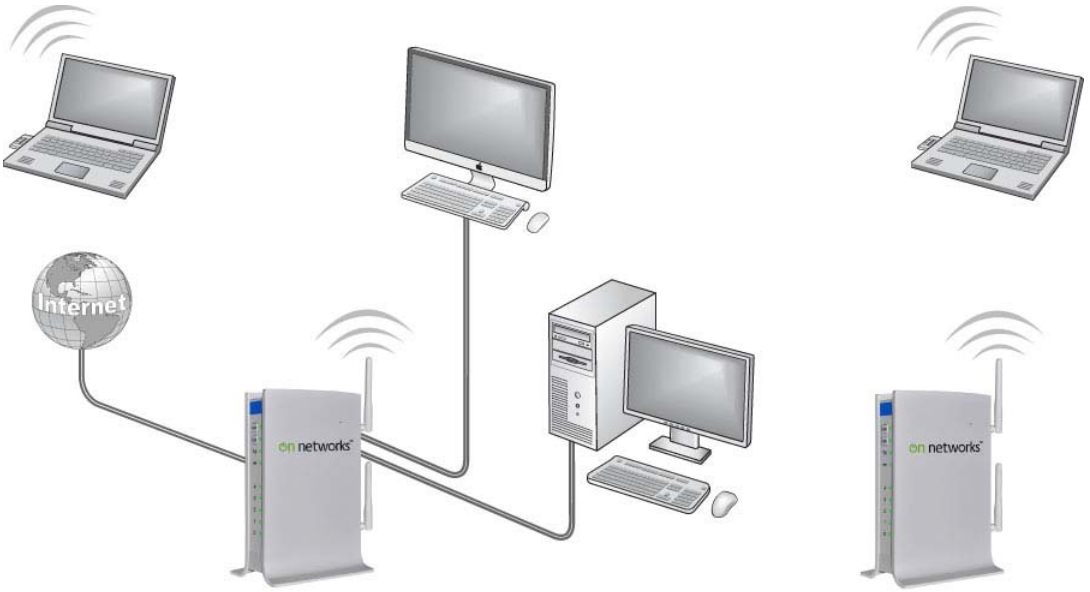


Abbildung 9. WLAN-Repeating-Szenario

Bei Verwendung der WLAN-Repeating-Funktion müssen Sie als Sicherheitsoption entweder WEP oder None (Keine) im Bildschirm **Wireless Settings** (Wireless-Konfiguration) auswählen. Die WEP-Option wird nur dann angezeigt, wenn Sie als WLAN-Modus im Bildschirm **Wireless Settings** (Wireless-Konfiguration) die Option Up to 54 Mbps (Bis zu 54 MBit/s) ausgewählt haben.

Wireless Base Station (WLAN-Basisstation): Der Modemrouter fungiert als übergeordneter Access Point, der den Datenverkehr zum und vom untergeordneten Repeater Access Point weiterleitet. Die Basisstation verwaltet zudem die über WLAN und Kabel verbundenen lokalen Computer. Zur Konfiguration dieses Modus benötigen Sie die MAC-Adressen des untergeordneten Repeater Access Points.

Wireless Repeater (WLAN-Repeater): Der Modemrouter sendet den gesamten Datenverkehr von den über WLAN und Kabel verbundenen Computern zu einem Remote Access Point. Zur Konfiguration dieses Modus benötigen Sie die MAC-Adresse des übergeordneten Remote Access Points.

Der Modemrouter befindet sich im Dualband-Parallelmodus, solange das WLAN aktiviert ist. Die WLAN-Basisstation bzw. der WLAN-Repeater kann bei Aktivierung des WLAN-Repeaters in einem Frequenzband nicht für ein anderes Frequenzband aktiviert werden. Wenn Sie jedoch die WLAN-Basisstation in einem Frequenzband aktivieren und das andere Frequenzband als WLAN-Modemrouter oder WLAN-Basisstation verwenden, wirkt sich dies nicht auf den Dualband-Parallelmodus aus.

Damit Sie ein WLAN mit WDS konfigurieren können, müssen die folgenden Bedingungen für beide Access Points erfüllt sein:

- Beide Access Points müssen dieselbe SSID, denselben Funkkanal und denselben Verschlüsselungsmodus verwenden.
- Beide Access Points müssen sich im selben LAN-IP-Subnetz befinden. Das bedeutet, die LAN-IP-Adressen des Access Points müssen sich im selben Netzwerk befinden.
- Alle LAN-Geräte (über WLAN und Kabel mit dem Netzwerk verbundene Computer) sind für den Betrieb im selben LAN-Netzwerkadressbereich wie die Access Points konfiguriert.

WLAN-Repeating

➢ **So zeigen Sie die Konfiguration von WLAN-Repeating an oder ändern diese:**

Wählen Sie **Advanced** (Erweitert) > **Wireless Repeating Function** (WLAN-Repeating) aus.

Dieser Bildschirm enthält die folgenden Einstellungen:

- **Enable Wireless Repeating Function** (WLAN-Repeating aktivieren): Aktivieren Sie dieses Kontrollkästchen, um WLAN-Repeating zu verwenden.
- **Disable Wireless Client Association** (WLAN-Client-Zuordnung deaktivieren): Wenn der Modemrouter die Rolle des Repeaters übernimmt, führt die Aktivierung dieses Kontrollkästchens dazu, dass die WLAN-Clients sich nicht verbinden können. Nur LAN-Client-Zuordnungen sind zulässig.
  - Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Punkt-zu-Punkt-Verbindung konfigurieren.
  - Aktivieren Sie dieses Kontrollkästchen dagegen nicht, wenn der gesamte Client-Datenverkehr über den anderen Access Point (Repeater mit WLAN-Client-Zuordnung) weitergeleitet werden soll.

- **Wireless MAC of this Router** (WLAN-MAC-Adresse dieses Routers): In diesem Feld wird die MAC-Adresse des Modemrouters zu Ihrer Information angezeigt. Sie müssen die MAC-Adresse in den entsprechenden Bildschirm für das WLAN-Repeating des anderen verwendeten Access Points eingeben.
- **Wireless Repeater** (WLAN-Repeater): Aktivieren Sie diese Optionsschaltfläche, wenn der Modemrouter die Rolle des Repeaters übernimmt.

  Repeater IP Address (Repeater-IP-Adresse): Geben Sie die IP-Adresse des anderen Access Points ein, wenn der Modemrouter die Rolle des Repeaters übernimmt.

  Base Station MAC Address (MAC-Adresse der Basisstation): Geben Sie die MAC-Adresse des Access Points ein, der als Basisstation dient, wenn der Modemrouter die Rolle des Repeaters übernimmt.
- **Wireless Base Station** (WLAN-Basisstation): Aktivieren Sie diese Optionsschaltfläche, wenn der Modemrouter die Rolle der Basisstation übernimmt.

  Disable Wireless Client Association (WLAN-Client-Zuordnung deaktivieren): Wenn der Modemrouter die Rolle der Basisstation übernimmt, führt die Aktivierung dieses Kontrollkästchens dazu, dass die WLAN-Clients sich nicht verbinden können. Nur LAN-Client-Zuordnungen sind zulässig.

  Repeater MAC Address (Repeater-MAC-Adresse), 1 bis 4: Wenn der Modemrouter die Rolle der Basisstation übernimmt, kann er als „übergeordnete Instanz“ für bis zu 4 weitere Access Points fungieren. Geben Sie die MAC-Adressen der anderen Access Points in diese Felder ein.

Konfigurieren der Basisstation

WLAN-Repeating kann nur in einer Speichenarchitektur verwendet werden. Die einzelnen Geräte können nicht in einer Daisy Chain in Serie miteinander verbunden werden. Sie benötigen dazu die WLAN-Einstellungen von beiden Geräten. Außerdem müssen Sie die MAC-Adresse des Remote-Geräts kennen. Konfigurieren Sie zuerst die Basisstation und danach den Repeater.

➢ **So konfigurieren Sie die Basisstation:**

1. Konfigurieren Sie beide Geräte mit denselben WLAN-Einstellungen (SSID, Modus, Kanal und Sicherheitsoption). Als WLAN-Sicherheitsoption muss **None** (Keine) oder **WEP** ausgewählt werden.
2. Wählen Sie **Advanced** (Erweitert) > **Wireless Repeating Function** (WLAN-Repeating) aus.
3. Aktivieren Sie das Kontrollkästchen **Enable Wireless Repeating Function** (WLAN-Repeating aktivieren) und die Optionsschaltfläche **Wireless Base Station** (WLAN-Basisstation).
4. Geben Sie die MAC-Adresse von einem oder mehreren Repeatern ein.
5. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

Konfigurieren eines Repeaters

Konfigurieren Sie den Repeater über eine kabelgebundene Netzwerkverbindung, um Konflikte mit der WLAN-Verbindung zur Basisstation zu vermeiden.

Hinweis: Wenn Sie die N300RM Basisstation mit einem Router einer anderen Marke als der des Repeaters verwenden, müssen Sie möglicherweise weitere Konfigurationseinstellungen ändern. Insbesondere sollten Sie die DHCP-Serverfunktion des Wireless Repeater APs deaktivieren.

➢ **So konfigurieren Sie den Modemrouter als Repeater:**

1. Melden Sie sich bei dem Modemrouter an, der die Rolle des Repeaters übernimmt.
2. Wählen Sie **Basic** (Grundeinstellungen) > **Wireless Settings** (Wireless-Konfiguration) aus, und stellen Sie sicher, dass die WLAN-Einstellungen vollständig mit denen der Basisstation übereinstimmen. Als WLAN-Sicherheitsoption muss **WEP** oder **None** (Keine) ausgewählt sein.
3. Wählen Sie **Advanced** (Erweitert) > **Wireless Repeating Function** (WLAN-Repeating) aus.
4. Aktivieren Sie das Kontrollkästchen **Enable Wireless Repeating Function** (WLAN-Repeating aktivieren) und die Optionsschaltfläche **Wireless Repeater** (WLAN-Repeater).
5. Füllen Sie das Feld für die Repeater-IP-Adresse aus. Diese IP-Adresse muss sich im selben Subnetz wie die Basisstation befinden, jedoch von der LAN-IP-Adresse der Basisstation unterscheiden.
6. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).
7. Prüfen Sie die Verbindungen in den LANs.

   Ein Computer in einem beliebigen WLAN- oder kabelgebundenen LAN-Segment des Modemrouters muss eine Verbindung mit dem Internet herstellen oder Dateien und Drucker für alle anderen über WLAN oder Kabel verbundenen Computer oder Server, die mit dem anderen Access Point verbunden sind, freigeben können.

Dynamisches DNS

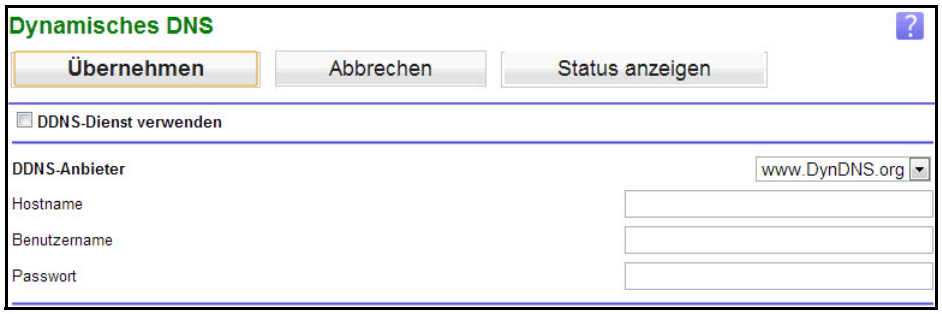
Wenn Ihr ISP (Internet-Provider) Ihrem Netzwerk eine permanente IP-Adresse zugewiesen hat, können Sie einen Domainnamen registrieren und diesen Namen über öffentliche Domain Name Server (DNS) mit Ihrer IP-Adresse verknüpfen lassen. Internetkonten werden meist dynamische IP-Adressen zugewiesen. Sie können nicht im Voraus sagen, wie Ihre IP-Adresse lauten wird. Zudem kann sich die Adresse häufig ändern. In diesem Fall können Sie einen kommerziellen dynamischen DNS-Dienst nutzen. Bei diesem Diensttyp können Sie Ihre Domain unter der IP-Adresse dieses Anbieters registrieren und für Ihre Domain bestimmten Datenverkehr an Ihre aktuelle IP-Adresse weiterleiten lassen.

Wenn Ihr ISP private WAN-IP-Adressen vergibt (wie z. B. 192.168.x.x oder 10.x.x.x), funktioniert der dynamische DNS-Dienst nicht, da eine Internet-Weiterleitung an private Adressen nicht möglich ist.

Der Modemrouter enthält einen Client, der eine Verbindung mit dem von DynDNS.org bereitgestellten dynamischen DNS-Dienst herstellen kann. Wenn Sie ein Konto eröffnen und Ihren Modemrouter einrichten, kontaktiert Ihr Modemrouter bei jedem Wechsel der IP-Adresse automatisch Ihren Anbieter für dynamische DNS-Dienste, meldet sich bei Ihrem Konto an und registriert Ihre neue IP-Adresse. Falls Ihr Hostname beispielsweise „hostname“ lautet, können Sie den Modemrouterunter http://hostname.dyndns.org erreichen.

➢ **So konfigurieren Sie dynamisches DNS:**

1. Richten Sie ein Konto bei einem der Anbieter für dynamische DNS-Dienste ein, dessen URLs in der Liste **Service Provider** (Dienstanbieter) angezeigt werden.
2. Klicken Sie auf **Advanced** (Erweitert) > Dynamic DNS (Dynamisches DNS).



3. Aktivieren Sie das Kontrollkästchen **Use a Dynamic DNS Service** (DDNS-Dienst verwenden).
4. Wählen Sie die URL Ihres DDNS-Anbieters aus. Wählen Sie für DynDNS.org beispielsweise **www.dyndns.org** aus.
5. Geben Sie den Hostnamen (oder Domainnamen) ein, der Ihnen vom DDNS-Anbieter zugewiesen wurde.
6. Geben Sie den Benutzernamen für Ihr DDNS-Konto ein. Dabei handelt es sich um den Namen für die Anmeldung bei Ihrem Konto, nicht um Ihren Hostnamen.
7. Geben Sie das Passwort (oder den Schlüssel) für Ihr DDNS-Konto ein.
8. Klicken Sie auf **Apply** (Übernehmen), um die Konfiguration zu speichern.

Statische Routen

Statische Routen liefern Ihrem Modemrouter zusätzliche Routinginformationen. In der Regel müssen Sie keine statischen Routen hinzufügen. Statische Routen müssen nur in Ausnahmefällen festgelegt werden, z. B. wenn Ihr Netzwerk mehrere Modemrouter oder IP-Subnetze enthält.

Im Folgenden finden Sie ein Beispiel für einen Fall, der den Einsatz einer statischen Route erforderlich macht:

- Ihr Hauptinternetzugang erfolgt über ein Kabelmodem, das Sie mit dem Internet-Provider verbindet.
- Außerdem ist an Ihr Heimnetzwerk ein ISDN-Modemrouter angeschlossen, über den Sie eine Verbindung zu dem Unternehmen, für das Sie arbeiten, aufbauen. Die Adresse dieses Modemrouter in Ihrem LAN lautet 192.168.0.100.
- Die Netzwerkadresse des Unternehmens ist 134.177.0.0.

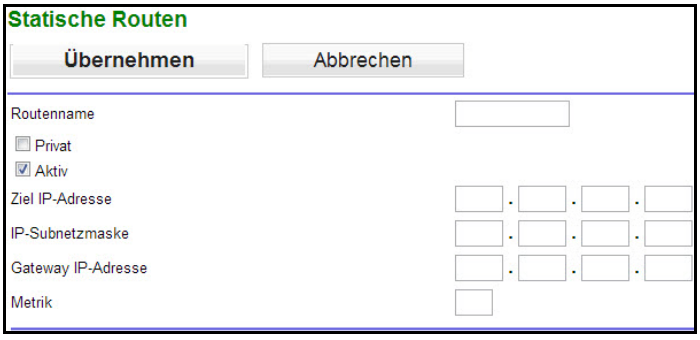
Bei der Anfangskonfiguration des Modemrouters wurden zwei statische Routen erstellt. Es wurden eine Standardroute mit Ihrem Internet-Provider als Gateway eingerichtet sowie eine zweite statische Route zu Ihrem lokalen Netzwerk für sämtliche Adressen des Typs 192.168.0.x. Wenn Sie versuchen, mit dieser Konfiguration auf ein Gerät im Netzwerk 134.177.0.0 zuzugreifen, leitet Ihr Modemrouter diese Anforderung an den ISP weiter. Der ISP gibt diese Anforderung an das Unternehmen, für das Sie arbeiten, weiter, wo sie wahrscheinlich von der Unternehmensfirewall abgelehnt wird.

In diesem Fall müssen Sie eine statische Route festlegen, die den Modemrouter dazu veranlasst, über den ISDN-Modemrouter mit der Adresse 192.168.0.100 auf die Adresse 134.177.0.0 zuzugreifen. In diesem Beispiel gilt:

- Die Einträge in den Feldern **Destination IP Address** (Ziel IP-Adresse) und **IP Subnet Mask** (IP-Subnetzmaske) legen fest, dass diese statische Route für alle Adressen des Typs 134.177.x.x gilt.
- Der Wert im Feld **Gateway IP Address** (Gateway IP-Adresse) gibt an, dass der gesamte Datenverkehr für diese Adressen an den ISDN-Modemrouter mit der Adresse 192.168.0.100 weitergeleitet werden soll.
- Im Feld **Metric** (Metrik) kann **1** stehen, da der ISDN-Modemrouter sich innerhalb des LANs befindet.
- **Private** (Privat) wurde nur als Vorsichtsmaßnahme ausgewählt, falls RIP aktiviert ist.

➢ **So konfigurieren Sie eine statische Route:**

1. Wählen Sie **Advanced** (Erweitert) > **Static Routes** (Statische Routen) aus, und klicken Sie auf **Add** (Hinzufügen), um den folgenden Bildschirm anzuzeigen:



2. Geben Sie in das Feld **Route Name** (Routenname) einen Namen für diese statische Route ein (nur zu Identifikationszwecken).

3. Aktivieren Sie das Kontrollkästchen **Private** (Privat), wenn Sie den Zugriff auf das LAN beschränken möchten. Bei Aktivierung der Option **Private** (Privat) wird die statische Route nicht im RIP angegeben.
4. Aktivieren Sie das Kontrollkästchen **Active** (Aktiv), um diese Route zu aktivieren.
5. Geben Sie die Ziel IP-Adresse des Zielhosts für die Route ein.
6. Geben Sie die IP-Subnetzmaske für das Ziel ein. Wenn es sich dabei um einen einzelnen Host handelt, geben Sie **255.255.255.255** als Ziel ein.
7. Geben Sie die Gateway IP-Adresse ein; hierbei muss es sich um einen Modemrouter im selben LAN-Segment wie der Modemrouter handeln.
8. Geben Sie im Feld **Metric** (Metrik) einen Wert aus dem Bereich 1 bis 15 ein.

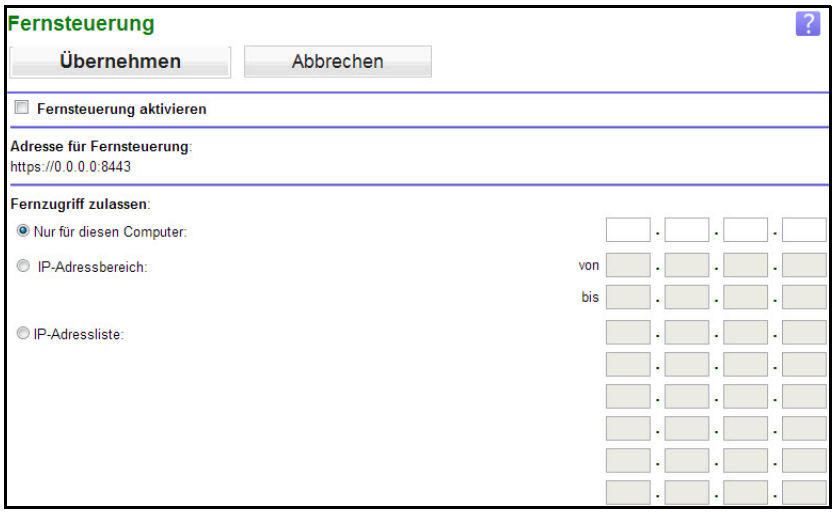
   Dieser Wert steht für die Anzahl der Modemrouter zwischen Ihrem Netzwerk und dem Ziel. In der Regel funktionieren die Werte 2 und 3; bei direkten Verbindungen sollte jedoch immer der Wert 1 gewählt werden.
9. Klicken Sie auf **Apply** (Übernehmen), um die statische Route hinzuzufügen.

Fernsteuerung

Mit der Fernsteuerung können Sie den Status des N300RM Modemrouters über das Internet aktualisieren oder prüfen.

➢ **So richten Sie die Fernsteuerung ein:**

1. Wählen Sie **Advanced** (Erweitert) > **Remote Management** (Fernsteuerung) aus.



Hinweis: *Ersetzen Sie das Standard-Anmeldepasswort des Modemrouters unbedingt durch ein sicheres Passwort. Das ideale Passwort enthält keine Wörter aus Wörterbüchern jeglicher Sprache und besteht aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Es kann aus bis zu 30 Zeichen bestehen.*

2. Aktivieren Sie das Kontrollkästchen **Turn Remote Management On** (Fernsteuerung aktivieren).
3. Geben Sie unter **Allow Remote Access By** (Fernzugriff zulassen) die externen IP-Adressen an, die auf die -Fernsteuerung zugreifen können.Modemrouter

Hinweis: Aus Sicherheitsgründen sollte der Fernzugriff auf einige wenige externe IP-Adressen beschränkt bleiben.

- Wenn nur eine einzige IP-Adresse im Internet die Zugriffsrechte erhalten soll, wählen Sie **Only This Computer** (Nur für diesen Computer). Geben Sie die IP-Adresse ein, die die Zugriffsrechte erhalten soll.
- Wenn nur IP-Adressen eines bestimmten Bereichs Zugriffsrechte erhalten sollen, wählen Sie **IP Address Range** (IP-Adressbereich). Geben Sie eine erste und eine letzte IP-Adresse ein, um den Bereich erlaubter Adressen festzulegen.
- Um die IP-Adressen anzugeben, wählen Sie **IP Address List** (IP-Adressliste) aus, und geben Sie die zulässigen IP-Adressen ein.
- Wenn jede beliebige IP-Adresse im Internet Zugriffsrechte erhalten soll, wählen Sie **Everyone** (Uneingeschränkt).

4. Geben Sie die Portnummer für den Zugriff auf die Internet-Benutzeroberfläche an.

   Dem normalen Zugriff über einen Webbrowser ist der Standard-HTTP-Dienstport 80 zugewiesen. Zur Erhöhung der Sicherheit können Sie eine benutzerdefinierte Portnummer für den Fernzugriff per Internet auf den Router eingeben. Wählen Sie eine Nummer im Bereich 1024 bis 65535. Verwenden Sie jedoch keine Standard-Portnummern gängiger Internetdienste. Als Standardwert ist 8080 eingestellt, ein gängiges Alias für HTTP.

5. Klicken Sie auf **Apply** (Übernehmen), um die Änderungen an den Router zu übermitteln.
6. Um über das Internet auf den Modemrouter zugreifen zu können, müssen Sie die WAN-IP-Adresse des Modemrouters in die Adressleiste des Webbrowsers eingeben, gefolgt von einem Doppelpunkt (:) und der benutzerdefinierten Portnummer. Angenommen, die derzeitige externe IP-Adresse Ihres Routers lautet 134.177.0.123 und Sie verwenden Portnummer 8080. Dann müssen Sie im Browser **http://134.177.0.123:8080** eingeben.

Universal Plug and Play

Universal Plug and Play (UPnP) vereinfacht den Netzwerkzugriff und die Vernetzung von Geräten aller Art, beispielsweise von Internet-Geräten und Computern. UPnP-fähige Geräte erkennen die von anderen registrierten UPnP-Geräten im Netzwerk angebotenen Dienste automatisch.

Wenn Sie Anwendungen wie Multi-Player-Games, Peer-to-Peer-Verbindungen und Echtzeitkommunikation (z. B. Instant Messaging oder die Remoteunterstützung von Windows XP) verwenden, sollten Sie UPnP aktivieren.

➢ **So aktivieren Sie Universal Plug and Play:**

1. Klicken Sie auf **Advanced** (Erweitert) > **UPnP**. Der Bildschirm **UPnP** wird angezeigt.

2. Legen Sie die Einstellungen fest.

   Auf diesem Bildschirm sind die folgenden Einstellungen und Informationen verfügbar:

   Turn UPnP On (UPnP aktivieren): Die automatische Gerätekonfiguration per UPnP kann aktiviert oder deaktiviert werden. Standardmäßig ist UPnP deaktiviert. Wenn dieses Kontrollkästchen nicht aktiviert ist, lässt der Modemrouter nicht zu, dass andere Geräte die Ressourcen des Modemrouters (wie z. B. die Portweiterleitung/Portzuordnung) automatisch steuern.

   Advertisement Period (Advertising-Lebensdauer): Die Advertising-Lebensdauer bestimmt, wie oft die UPnP-Daten des Modemrouters per Broadcast gesendet werden. Hier können Werte im Bereich 1 bis 1440 Minuten angegeben werden. Der Standardwert ist 30 Minuten. Kürzere Perioden stellen sicher, dass die Steuerungspunkte über aktuelle Informationen zum Gerätestatus verfügen, führen jedoch zu einem erhöhten Datenverkehr im Netzwerk. Bei längeren Perioden werden die Gerätestatusinformationen weniger oft aktualisiert; dafür verringert sich jedoch der Datenverkehr im Netzwerk erheblich.

   Advertisement Time to Live (Advertising-Lebensdauer): Die Advertising-Lebensdauer wird in Hops (Schritten) für jedes gesendete UPnP-Paket gemessen. Die Lebensdauer gibt die maximale Anzahl von Hops für die Weitergabe eines Broadcast-Pakets beim UPnP-Advertising an. Für die Anzahl der Hops können Werte im Bereich 1 bis 255 angegeben werden. Der Standardwert für die Advertising-Lebensdauer ist 4 Hops. Für Netzwerke in Privathaushalten ist dieser Wert in der Regel ausreichend. Wenn Sie feststellen, dass einige Geräte nicht aktualisiert oder nicht erreicht werden, sollten Sie einen höheren Wert wählen.

   UPnP Portmap Table (UPnP-Portzuordnungstabelle): In der UPnP-Portzuordnungstabelle werden die IP-Adressen aller aktuell auf den Modemrouter zugreifenden UPnP-Geräte und die von diesen geöffneten Ports (intern und extern) angezeigt. Darüber hinaus können Sie der UPnP-Portzuordnungstabelle die Typen der geöffneten Ports und deren Status (d. h. ob diese für die einzelnen IP-Adressen noch aktiv sind) entnehmen.

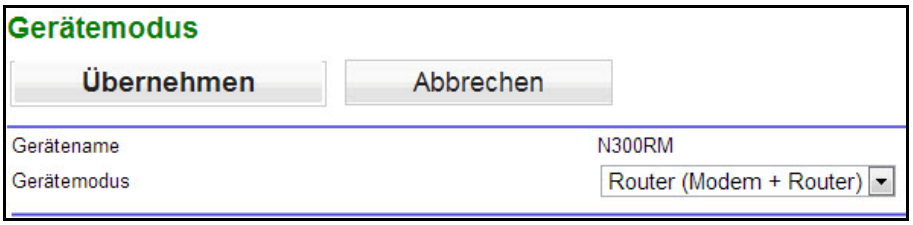
3. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Ändern des Gerätemodus

Das Modem enthält ein integrierten Router. Wenn Sie das Modem als Bridge im Modem-Modus konfigurieren wollen, müssen Sie zuerst die Internetverbindung einrichten und dann den Gerätemodus auf Modem-Modus setzen. Im Modem-Modus verhält sich das Gerät als Bridge oder DSL-Modem. Wenn sich das Gerät im Modem-Modus befindet, werden die nicht verfügbaren Funktionen ausgeblendet.

➢ **So ändern Sie den Gerätemodus:**

1. Wählen Sie **Advanced** (Erweitert) > **Device Mode** (Gerätemodus). Der folgende Bildschirm wird angezeigt:



   Standardmäßig befindet sich das Modem im Router-Modus.

2. Wählen Sie den gewünschten Gerätemodus aus der Dropdown-Liste aus.
3. Klicken Sie auf **Apply** (Übernehmen), damit die Änderungen wirksam werden.

Virtual Private Networking

7

VPN-Einrichtung

Dieses Kapitel enthält die folgenden Abschnitte:

- *Erstellen einer Gateway-zu-Gateway VPN-Konfiguration*
- *VPN-Assistent*
- *Aktivieren eines VPN-Tunnels*
- *Prüfen des Status eines VPN-Tunnels*
- *Konfiguration von VPN-Tunneln mithilfe der automatischen Regel*
- *Konfiguration von VPN-Tunneln mithilfe der manuellen Regel*

Erstellen einer Gateway-zu-Gateway VPN-Konfiguration

Zwei übliche Szenarien für VPN-Tunnel sind eine Verbindung zwischen einem Remote-Computer mit einem Netzwerk-Gateway oder zwischen zwei oder mehr Netzwerk-Gateways. Gateway-zu-Gateway VPN-Tunnel sorgen für einen sicheren netzwerkübergreifenden Zugriff, z.B. zwischen einer Niederlassung oder dem Heimbüro und einem Hauptbüro.

Ein VPN zwischen zwei oder mehreren VPN-fähigen Routern ist eine gute Möglichkeit, Neben- oder Heimbüros und Geschäftspartner über das Internet miteinander zu verbinden. VPN-Tunnel ermöglichen ferner den Zugriff auf Netzwerkressourcen im gesamten Internet. Bilden Sie dazu mithilfe der Gateways an jedem Tunnelende die Endpunkte der VPN-Tunnel.

Setzen Sie die LAN-IPs an jedem Modemrouter auf ein anderes Subnetz, und nehmen Sie die richtigen Internetkonfigurationen vor. Die folgende Tabelle zeigt ein Beispiel:

Tabelle 3. Konfiguration von Gateway-zu-Gateway VPN-Tunneln

Parameter		**Einzugebender Wert**	**Feldabschnitt**	
Connection Name (Verbindungsname)		GtoGr	-	
Pre-Shared Key		12345678	-	
Sicherheitsvereinbarung		-	Hauptmodus	Manuelle Schlüssel
Perfect Forward Secrecy		-	Aktiviert	Deaktiviert
Verschlüsselungsprotokoll		-	DES	3DES
Authentifizierungsprotokoll		-	MD5	SHA-1
Diffie-Hellman-Gruppe		-	Gruppe 1	Gruppe 2
Gültigkeit des Schlüssels in Sekunden		28800 (8 Stunden)	-	
IKE-Lebensdauer in Sekunden		3600 (1 Stunde)	-	
VPN-Endpunkt	**Local IPSecID**	**LAN-IP-Adresse**	**Subnet Mask (Subnetzmaske)**	**FQDN- oder Gateway-IP (WAN-IP-Adresse)**
Gateway_A	GW_A	192.168.0.1	255.255.255.0	14.15.16.17
Gateway_B	GW_B	192.168.3.1	255.255.255.0	22.23.24.25

Die LAN-IP-Adressbereiche für die VPN-Endpunkte müssen unterschiedlich sein. Die Verbindung schlägt fehl, wenn beide den Standard-Adressbereich 192.168.0.x verwenden.

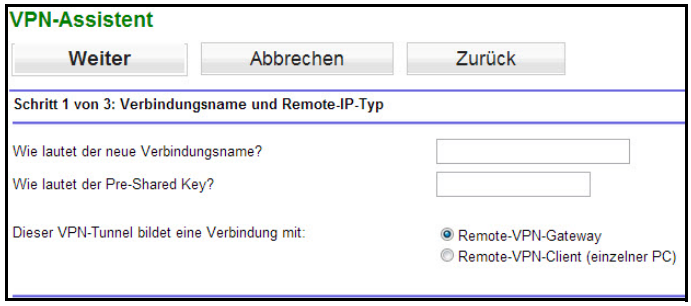
VPN-Assistent

Der VPN-Assistent führt Sie durch die Konfiguration des VPN-Tunnels, wobei viele der Schritte automatisch durchgeführt werden. Wenn Sie den VPN-Assistenten nicht benutzen möchten bzw. dessen Standardeinstellungen für Sie nicht geeignet sind, wählen Sie eine der folgenden Alternativen:

- **Auto Policy** (Automatische Regel): Die automatische Regel definiert das Authentifizierungschema und erstellt die Datenschlüssel automatisch anhand des IKE-Protokolls. Siehe *Konfiguration von VPN-Tunneln mithilfe der automatischen Regel* auf Seite 96.
- **Manual Policy** (Manuelle Regel): Geben Sie alle Authentifizierungs- und Schlüsselparameter manuell ein. Siehe *Konfiguration von VPN-Tunneln mithilfe der manuellen Regel* auf Seite 100.

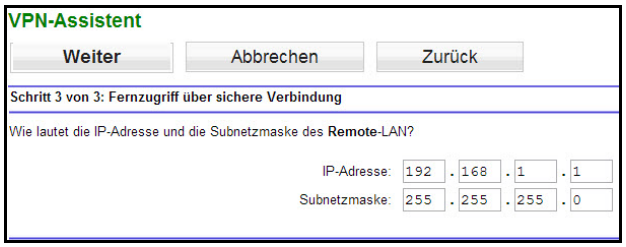
➢ **So konfigurieren Sie einen Gateway-zu-Gateway VPN-Tunnel mithilfe des VPN-Assistenten:**

1. Wählen Sie **Advanced > VPN Wizard** (Erweitert > VPN-Assistent), und klicken Sie auf **Next** (Weiter).
2. Tragen Sie den Verbindungsnamen und den Pre-Shared-Key in die entsprechenden Felder ein.

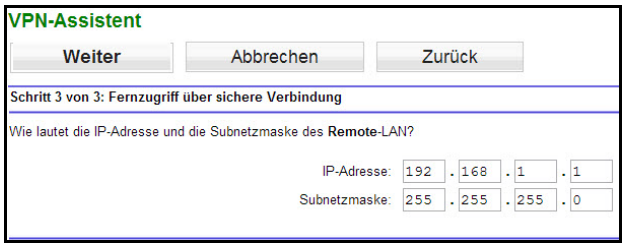


3. Wählen Sie die Optionsschaltfläche **A remote VPN Gateway** (Remote-VPN-Gateway), und klicken Sie auf **Next** (Weiter).
4. Tragen Sie die IP-Adresse oder FQDN für die WAN-Verbindung des VPN-Zielendpunkts ein, und klicken Sie auf **Next** (Weiter.)

5. Tragen Sie die IP-Adresse und die Subnetzmaske des Zielendpunkts, der diesen Tunnel nutzen kann, in die entsprechenden Felder ein, und klicken Sie auf **Next** (Weiter).


VPN-Assistent
Weiter
Abbrechen
Zurück
Schritt 3 von 3: Fernzugriff über sichere Verbindung
Wie lautet die IP-Adresse und die Subnetzmaske des Remote-LAN?
IP-Adresse: 192 . 168 . 1 . 1
Subnetzmaske: 255 . 255 . 255 . 0

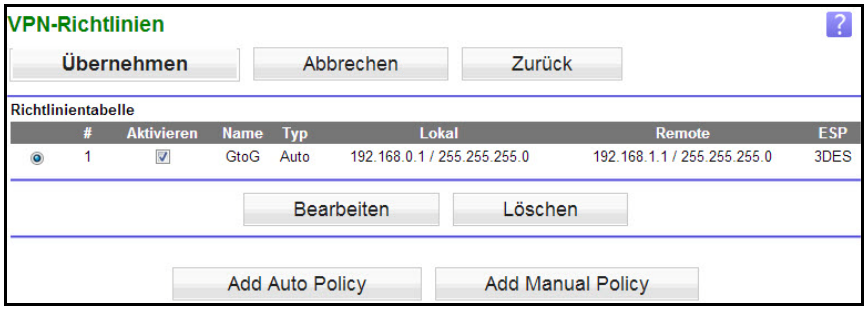
6. Bestimmen Sie die lokale LAN-Adresse und die Subnetzmaske. Klicken Sie anschließend auf **Next** (Weiter).


VPN-Assistent
Weiter
Abbrechen
Zurück
Schritt 3 von 3: Fernzugriff über sichere Verbindung
Wie lautet die IP-Adresse und die Subnetzmaske des Remote-LAN?
IP-Adresse: 192 . 168 . 1 . 1
Subnetzmaske: 255 . 255 . 255 . 0

Der Bildschirm **VPN Wizard Summary** (Zusammenfassung für den VPN-Assistenten) öffnet sich:

7. Klicken Sie auf **Done** (Fertig).

   Es öffnet sich der Bildschirm **VPN Policies** (VPN-Richtlinien) und zeigt an, dass der neue Tunnel aktiviert ist.



8. Wiederholen Sie diese Schritte für das zweite Gateway. Achten Sie dabei besonders auf folgende Netzwerkeinstellungen:
   - WAN-IP des Remote-VPN-Gateways (z. B. **14.15.16.17**)
   - Konfiguration der LAN-IP für das Remote-VPN-Gateway:
     - IP-Adresse (z. B. **192.168.0.1**)
     - Subnetzmaske (z. B. **255.255.255.0**)
     - Pre-Shared Key (z. B.**12345678**)

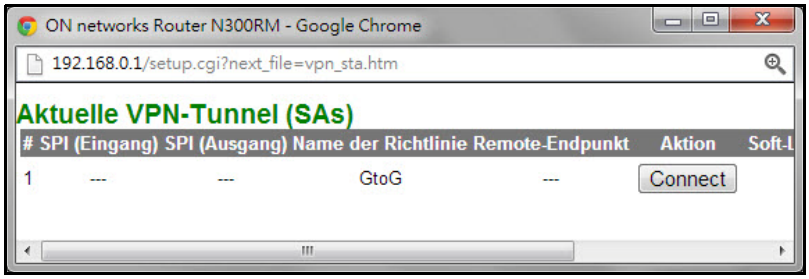
Aktivieren eines VPN-Tunnels

Es gibt drei Möglichkeiten, den VPN-Tunnel zu aktivieren:

- Über den Bildschirm **VPN Status** (VPN-Status).
- Senden eines Ping-Signals an den Remote-Endpunkt.
- Erste Benutzung des VPN-Tunnels.

➢ **So aktivieren Sie einen VPN-Tunnel über den VPN-Status-Bildschirm:**

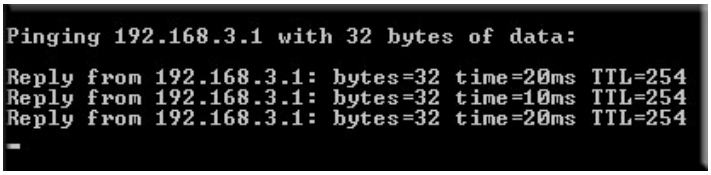
1. Wählen Sie **Advanced > VPN Status** (Erweitert > VPN-Status).
2. Klicken Sie auf **VPN Status** (VPN-Status) um den Bildschirm **Current VPN Tunnels (SAs)** (Aktuelle VPN-Tunnel [SAs]) zu öffnen:


ON networks Router N300RM - Google Chrome
192.168.0.1/setup.cgi?next_file=vpn_sta.htm
Aktuelle VPN-Tunnel (SAs)
SPI (Eingang) SPI (Ausgang) Name der Richtlinie Remote-Endpunkt Aktion Soft-L
1 --- --- GtoG --- Connect

3. Klicken Sie bei dem VPN-Tunnel, den Sie aktivieren möchten, auf **Connect** (Verbinden). Prüfen Sie im Bildschirm **VPN Status/Log** (VPN-Status/Protokoll), ob eine Verbindung zum Tunnel vorhanden ist.

➢ **So aktivieren Sie den VPN-Tunnel über ein Ping-Signal an dem Remote-Endpunkt:**

1. Prüfen Sie den VPN-Tunnel, indem Sie von einem an Gateway A (Modemrouter) angeschlossenen Computer ein Ping-Signal an das Remote-Netzwerk senden.
2. Öffnen Sie das Befehlsfeld (über **Start > Run > cmd** (Start > Ausführen > cmd)).
3. Geben Sie **ping 192.168.3.1** ein (der Endpunkt Ihres Remote-Gateways wird ersetzt).


Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=10ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254

Der Pingvorgang kann beim ersten Mal fehlschlagen. Versuchen Sie es in dem Fall ein zweites Mal.

➢ **So aktivieren Sie einen VPN-Tunnel über einen VPN-Tunnel:**

Öffnen Sie in Ihrem Browser eine URL, deren IP-Adresse oder Bereich von den Regeln des VPN-Tunnels abgedeckt wird, um einen VPN-Tunnel zu verwenden.

Prüfen des Status eines VPN-Tunnels

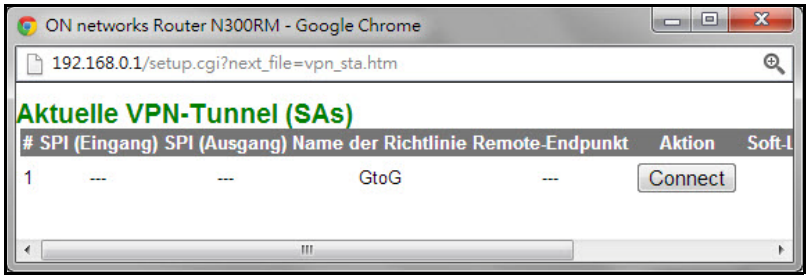
Der Bildschirm **VPN Status** (VPN-Status) enthält ein Protokoll, das die Einzelheiten zu den letzten VPN-Aktivitäten, einschließlich dem Aufbau des VPN-Tunnels, anzeigt. Wenn ein Problem mit dem VPN-Tunnel vorliegt, finden Sie im Protokoll Informationen zur möglichen Ursache des Problems.

➢ **So überprüfen Sie den VPN-Tunnel-Status:**

1. Wählen Sie **Advanced > VPN Status** (Erweitert > VPN-Status).

   Klicken Sie auf die Optionsschaltfläche **Refresh** (Aktualisieren), um die letzten Einträge anzuzeigen. Klicken Sie auf **Clear Log** (Protokoll löschen), um alle Einträge aus dem Protokoll zu löschen.

2. Klicken Sie auf **VPN Status** (VPN-Status), um den Bildschirm **Current VPN Tunnels (SAs)** (Aktuelle VPN-Tunnel [SAs]) zu öffnen.


ON networks Router N300RM - Google Chrome
192.168.0.1/setup.cgi?next_file=vpn_sta.htm
Aktuelle VPN-Tunnel (SAs)
SPI (Eingang) SPI (Ausgang) Name der Richtlinie Remote-Endpunkt Aktion Soft-L
1 --- --- GtoG --- Connect

Diese Tabelle enthält die nachstehenden Daten für alle aktiven VPN-Tunnel.

- **SPI**: Jede Sicherheitsvereinbarung (SA) besitzt einen eindeutigen Sicherheitsparameterindex (Security Parameter Index, SPI) für den Datenverkehr in jede Richtung. Beim manuellen Schlüsselaustausch ist der SPI in der Richtliniendefinition festgelegt. Beim automatischen Schlüsselaustausch wird er durch das IKE-Protokoll erzeugt.
- **Policy Name** (Name der Richtlinie): Die aktuelle, mit dieser SA verknüpfte VPN-Richtlinie.
- **Remote Endpoint** (Remote-Endpunkt): IP-Adresse des Remote-VPN-Endpunkts.
- **Action** (Aktion): Entweder eine Schaltfläche Drop (Trennen) oder Connect (Verbinden).
- **SLifeTime (Secs)** (SLebensdauer [Sekunden]): Die verbleibende Software-Lebensdauer für diese Sicherheitsvereinbarung (SA) in Sekunden. Sobald die Software-Lebensdauer auf Null sinkt, wird die Sicherheitsvereinbarung (Security Association, SA) neu ausgehandelt.
- **HLifeTime (Secs)** (HLebensdauer [Sekunden]): Die verbleibende Hardware-Lebensdauer für diese Sicherheitsvereinbarung (SA) in Sekunden. Bei einer Hardware-Lebensdauer von 0 (Null) wird die SA beendet. (Bei Bedarf kann die Vereinbarung wiederhergestellt werden.)

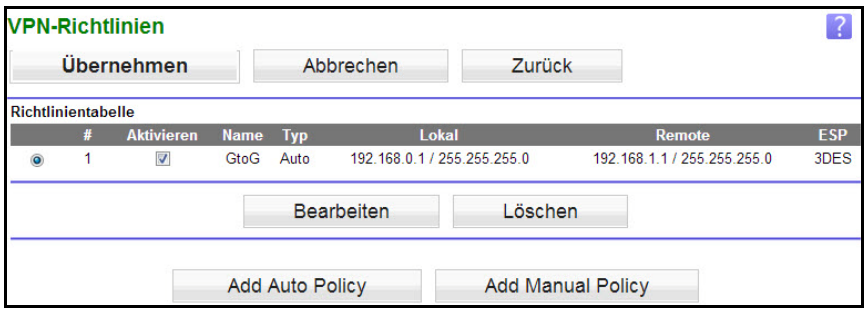
Deaktivieren eines VPN-Tunnels

In einigen Fällen müssen Sie einen VPN-Tunnel zu Testzwecken deaktivieren. Sie können dies über zwei Stellen tun:

- Über die Tabelle **Policy** (Regel) im Bildschirm **VPN Policies** (VPN-Richtlinien).
- Über den Bildschirm **VPN Status** (VPN-Status)

➢ **Um die Tabelle Policy (Regel) verwenden zu können, deaktivieren Sie den VPN-Tunnel wie folgt:**

1. Wählen Sie **Advanced > VPN Policies** (Erweitert > VPN-Richtlinien).

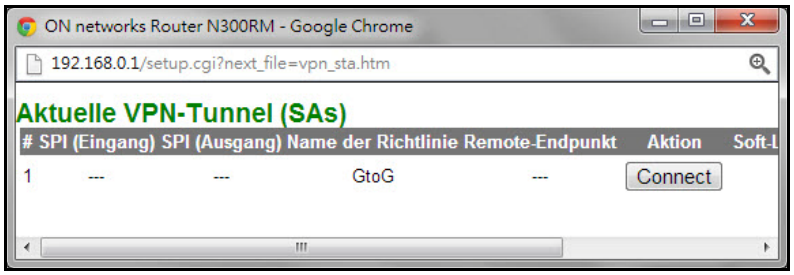


2. Deaktivieren Sie in der Tabelle **Policy** (Regel) die Option **Enable** (Aktivieren) für den VPN-Tunnel, den Sie deaktivieren möchten.
3. Klicken Sie auf **Apply** (Übernehmen).

Wählen Sie die Option **Enable** (Aktivieren), um den Tunnel wieder zu aktivieren, und klicken Sie auf **Apply** (Übernehmen).

➢ **So deaktivieren Sie einen VPN-Tunnel über den Bildschirm VPN Status (VPN-Status):**

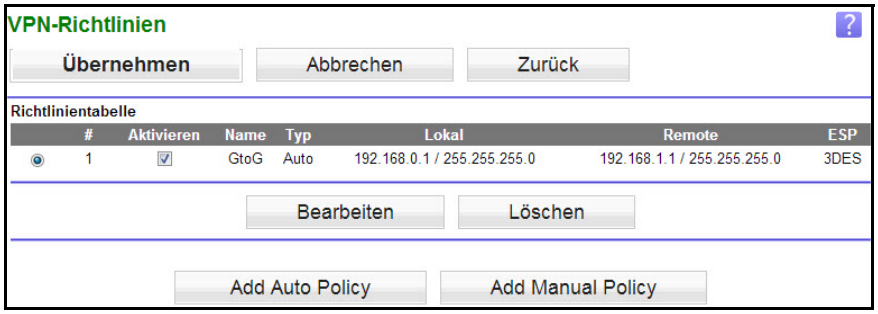
1. **Advanced > VPN Status** (Erweitert > VPN-Status).
2. Klicken Sie auf die Schaltfläche **VPN-Status** (VPN-Status).


ON networks Router N300RM - Google Chrome
192.168.0.1/setup.cgi?next_file=vpn_sta.htm
Aktuelle VPN-Tunnel (SAs)
SPI (Eingang) SPI (Ausgang) Name der Richtlinie Remote-Endpunkt Aktion Soft-L
1 --- --- GtoG --- Connect

3. Klicken Sie für den Tunnel, den Sie deaktivieren möchten, auf **Drop** (Trennen).

➢ **So deaktivieren Sie einen VPN-Tunnel:**

1. Wählen Sie **Advanced > VPN Policies** (Erweitert > VPN-Richtlinien).



2. Wählen Sie in der Tabelle **Policy** (Regel) die Option für den VPN-Tunnel, den Sie löschen möchten.
3. Klicken Sie auf **Delete** (Löschen).

Konfiguration von VPN-Tunneln mithilfe der automatischen Regel

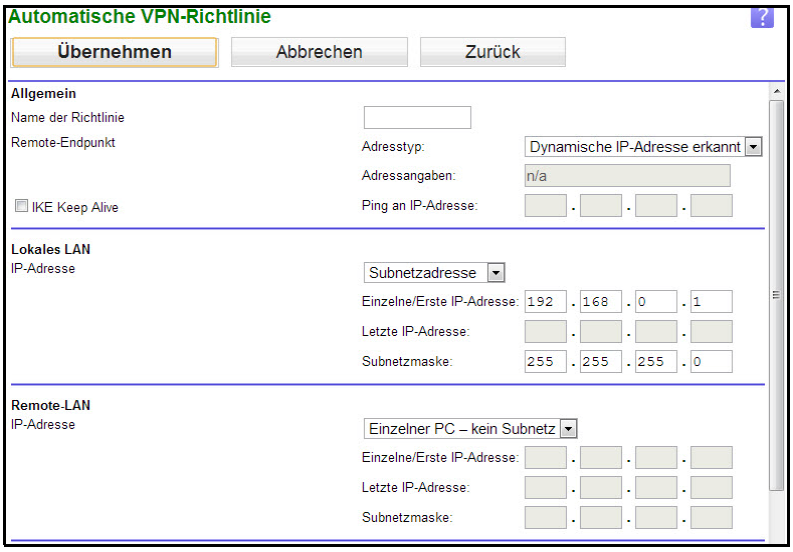
Sie müssen an beiden VPN-Endpunkten passende VPN-Einstellungen vornehmen. Die Einstellungen für das Ausgangs-VPN an einem Ende müssen den Einstellungen des Eingangs-VPN am anderen Ende entsprechen und umgekehrt.

Alle VPN-Tunnel des Modemrouters erfordern die Konfiguration verschiedener Netzwerk-Parameter. Dieses Kapitel beschreibt diese Parameter und wo Sie sie finden.

Die üblichsten Konfigurationen verwenden IKE zur Verwaltung der Authentifizierungs- und Datenschlüssel. Das IKE-Protokoll verhandelt zwischen den beiden VPN-Endpunkten, um die erforderlichen Verschlüsselungsparameter zu erstellen und zu aktualisieren.

➢ **So konfigurieren Sie VPN-Netzwerk-Parameter:**

1. Wählen Sie **Advanced > VPN Policies** (Erweitert > VPN-Richtlinien).
2. Klicken Sie auf **Add Auto Policy** (Automatische Regel hinzufügen).



Folgende Abschnitte enthalten die Felder mit den Netzwerkverbindungen für VPN-Tunnel.

Allgemeine Einstellungen für die automatische VPN-Richtlinie

- **Policy Name** (Name der Richtlinie): Geben Sie einen eindeutigen Namen ein. Dieser Name wird nicht an den Remote-VPN-Endpunkt übermittelt. Er dient lediglich zur Verwaltung der Richtlinien.
- **Remote VPN Endpoint** (Remote-VPN-Endpunkt): Als Remote-VPN-Endpunkt muss die Adresse des aktuellen VPN-Gateways angegeben werden.

  Wenn der Remote-Endpunkt über eine dynamische IP-Adresse verfügt, wählen Sie **Dynamic IP Address** (Dynamische IP-Adresse). Es muss keine Adresse angegeben werden. Sie können mehrere dynamische Remote-IP-Regeln erstellen, es kann aber immer nur eine Regel aktiviert werden. Oder wählen Sie eine Option aus (**IP address** (IP-Adresse) oder **domain name** (Domainname)), und geben Sie die Adresse bzw. den Namen des Remote-VPN-Endpunkts ein, zu dem Sie eine Verbindung herstellen möchten
- **IKE Keep Alive**: Aktivieren Sie diese Option, wenn eine Verbindung offen bleiben oder, falls dies nicht möglich ist, nach einer Trennung schnellstmöglich wiederhergestellt werden soll.

  Die IP-Adresse muss dem Remote-Endpunkt zugeordnet sein. Sie müssen die Remote-LAN-IP-Adresse verwenden. Zur Erzeugung von Datenverkehr im VPN-Tunnel wird regelmäßig ein Ping-Signal an die entsprechende IP-Adresse gesendet. Die IP-Adresse des Remote-Keep-Alive muss im IP-Bereich des Remote-LAN liegen und zu einem Gerät gehören, das auf das Ping-Signal antworten kann. Um dieses Ziel zu erreichen, sollte der Bereich so eng wie möglich gehalten werden.

Lokale LAN-Einstellungen für die automatische VPN-Richtlinie

Diese IP-Adressen müssen als Remote-Adressen für den Remote-VPN-Endpunkt eingegeben werden.

- **Subnet Mask** (Subnetzmaske): Die Netzwerkmaske.
- **Single/Start IP Address** (Einzelne/Erste IP-Adresse): Geben Sie die IP-Adresse für eine Einzeladresse ein, oder die erste Adresse für einen Adressbereich. Einzeladressen werden verwendet, wenn Sie Remote-Benutzern den Zugriff auf einen einzigen Server in Ihrem LAN ermöglichen möchten. Der Bereich muss dem Adressbereich Ihres LAN entsprechen.
- **Any** (Beliebig): Für den Remote-VPN-Endpunkt können Sie eine beliebige IP-Adresse eingeben.
- **Finish IP Address** (Letzte IP-Adresse): Geben Sie die letzte IP-Adresse für den Adressbereich ein. Der Bereich muss dem Adressbereich Ihres LAN entsprechen.

Remote-LAN-Einstellungen für VPN - Automatische Regel

Bei diesen IP-Adressen handelt es sich um die lokalen Adressen für den Remote-VPN-Endpunkt.

- **IP Address** (IP-Adresse): Wenn sich am Remote-Endpunkt nur ein einzelner Computer statt eines LAN befindet, wählen Sie die Option **Single PC - no Subnet** (Einzelne Adresse/ Kein Subnetz). Für diese Option sind keine weiteren Angaben erforderlich. Typischerweise ist dies der Computer, auf dem sich der VPN-Client am Remote-Ende befindet.
- **Single/Start IP Address** (Einzelne/Erste IP-Adresse): Geben Sie eine IP-Adresse ein, die auch im Remote-LAN enthalten ist. Über diese Einstellung kann auch auf einen Server im Remote-LAN zugegriffen werden.
  - Geben Sie bei einem Adressbereich die erste IP-Adresse ein. Der Adressbereich muss im Remote-LAN vorhanden sein.
  - **Any** (Beliebig): Jeglicher von Computern in den Feldern Local IP (Lokale IP-Adresse) abgehende Datenverkehr löst einen VPN-Verbindungsversuch zum Remote-VPN-Endpunkt aus. Stellen Sie sicher, dass Sie diese Option wirklich anwenden möchten, bevor Sie sie auswählen.
- **Finish IP Address** (Letzte IP-Adresse): Geben Sie die letzte IP-Adresse für einen Adressbereich ein. Der Adressbereich muss im Remote-LAN vorhanden sein.
- **Subnet Mask** (Subnetzmaske): Geben Sie die Netzwerkmaske ein.

IKE-Einstellungen für die automatische VPN-Richtlinie

- **Direction** (Richtung): Diese Einstellung wird verwendet, wenn der Modemrouter überprüft, ob die IKE-Regel dem aktuellen Datenverkehr entspricht. Wählen Sie eine Option.
  - **Responder only** (Nur Responder): Eingangsverbindungen werden zugelassen, Ausgangsverbindungen hingegen gesperrt.
  - **Initiator and Responder** (Initiator und Responder): Eingangs- sowie Ausgangsverbindungen werden zugelassen.
- **Exchange Mode** (Austauschmodus): Stellen Sie sicher, dass der Remote-VPN-Endpunkt im Main Modus (Hauptmodus) ist.

- **Diffie-Hellman (DH) Group** (Diffie-Hellman-Gruppe): Der Diffie-Hellman-Algorithmus wird zum Schlüsselaustausch verwendet. Mit der DH-Einstellung wird die beim Schlüsselaustausch verwendete Bitgröße festgelegt. Dieser Wert muss mit dem Wert für das Remote-VPN-Gateway übereinstimmen.
- **Local Identity Type** (Lokaler Kennungstyp): Wählen Sie die gewünschte Option, die den Einstellungen des Remote-Kennungstyps (siehe unten) am Remote-VPN-Endpunkt entspricht.
  - **WAN IP Address** (WAN-IP-Adresse): Ihre Internet IP-Adresse.
  - **Fully Qualified Domain Name**: Ihr Domainname.
  - **Fully Qualified User Name**: Ihr Name, Ihre E-Mail-Adresse und sonstige Kennung.
  - **Local Identity Data** (Lokale Kennungsdaten): Geben Sie die Daten für die gewählte lokale Kennung ein. (Für die Option **WAN IP Address** [WAN-IP-Adresse] ist keine Eingabe erforderlich.)
- **Remote Identity Type** (Remote-Kennungstyp): Wählen Sie die gewünschte Option, die den Einstellungen des lokalen Kennungstyps (siehe oben) am Remote-VPN-Endpunkt entspricht.
  - **IP Address** (IP-Adresse): Die Internet IP-Adresse des Remote-VPN-Endpunkts.
  - **Fully Qualified Domain Name**: Der Domainname des Remote-VPN-Endpunkts.
  - **Fully Qualified User Name**: Name, E-Mail-Adresse oder sonstige Kennung des Remote-VPN-Endpunkts.
  - **Remote Identity Data** (Remote-Kennungsdaten): Geben Sie die Daten für die gewählte Remote-Kennung ein. Für die IP-Adresse sind hier keine Angaben erforderlich.

Parameter für automatische VPN-Richtlinien

- **Encryption Algorithm** (Verschlüsselungsalgorithmus): Der für IKE und IPSec zu verwendende Verschlüsselungsalgorithmus. Diese Einstellung muss mit der Einstellung für das Remote-VPN-Gateway übereinstimmen. DES und 3DES werden unterstützt.
  - **DES**: Der Data Encryption Standard (DES) verarbeitet eingehende Daten mit einer Breite von 64 Bit und verschlüsselt diese Werte mit einem 56-Bit-Schlüssel. Schneller, aber nicht so sicher wie 3DES.
  - **3DES**: (3DES) erreicht einen höheren Sicherheitsgrad, indem es die Daten dreimal mit DES und drei unterschiedlichen, voneinander unabhängigen Schlüsseln verschlüsselt.
- **Authentication Algorithm** (Authentifizierungsalgorithmus): Der für IKE und IPSec zu verwendende Authentifizierungssalgorithmus. Diese Einstellung muss mit der Einstellung für das Remote-VPN-Gateway übereinstimmen. Auto, MD5, und SHA-1 werden unterstützt. Verhandelt automatisch mit dem Remote-VPN-Endpunkt und steht im Modus **Responder-only** (Nur Responder) nicht zur Verfügung.
  - **MD5**: 128 Bit, schneller, aber nicht so sicher
  - **SHA-1**: 160 Bit, langsamer, aber sicherer Das ist der Standardwert.
- **Pre-Shared Key**: Der Schlüssel muss hier und am Remote-VPN-Gateway eingegeben werden.

- **SA Life Time** (SA-Lebensdauer): Die Zeit bis zum Ablauf der Sicherheitsvereinbarung (Security Association, SA). (Sie wird bei Bedarf automatisch wiederhergestellt.) Eine kurze Zeitdauer (bzw. kleine Datenmenge) erhöht zwar die Sicherheit, verringert jedoch die Leistung. Übliche Werte für die SA-Lebensdauer liegen über einer Stunde (3600 Sekunden). Diese Einstellung gilt für Security Associations von IKE- sowie IPSec-Protokollen.
- **Enable IPSec PFS (Perfect Forward Secrecy)** (PFS (Perfect Forward Secrecy) für IPSec aktivieren): Durch Aktivieren dieser Option wird die Sicherheit durch regelmäßigen Schlüsselaustausch erhöht. Sollte ein Schlüssel geknackt werden, wird das Knacken der folgenden Schlüssel dadurch nicht vereinfacht. (Jeder Schlüssel wird unabhängig vom vorherigen Schlüssel generiert.)

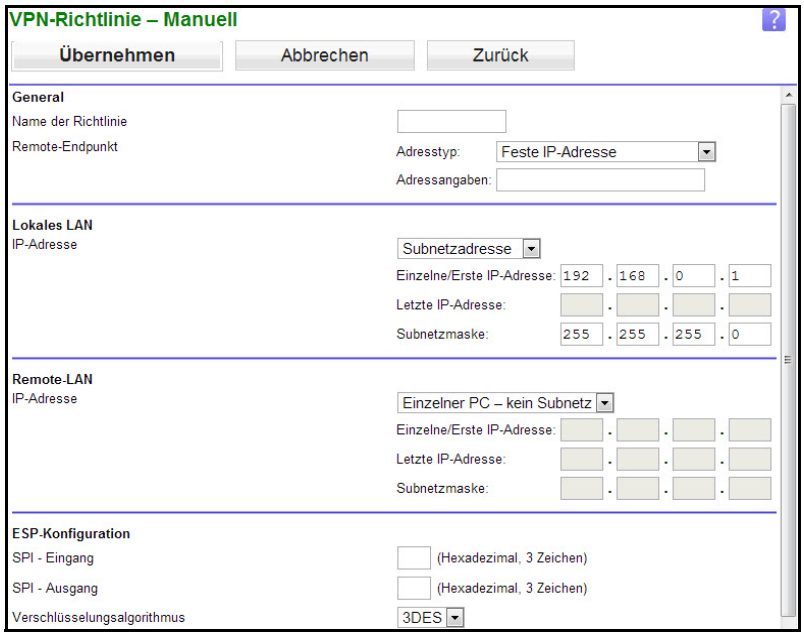
  Diese Einstellung gilt für Security Associations von IKE- sowie IPSec-Protokollen. Um die entsprechenden Einstellungen des Remote-Endpunkts anzupassen, müssen Sie u.U. die verwendete Schlüsselgruppe angeben. Dieses Gerät gehört zur der unter den IKE-Einstellungen festgelegten Diffie-Hellman-Gruppe.

Konfiguration von VPN-Tunneln mithilfe der manuellen Regel

Alternativ zu IKE können Sie manuelle Schlüssel verwenden, in denen jede Verbindungsphase festgelegt werden muss. Bei einer manuellen VPN-Regel müssen alle Einstellungen für den VPN-Tunnel manuell an beiden Enden (an beiden VPN-Endpunkten) eingegeben werden.

➢ **So erstellen Sie eine Regel manuell:**

1. Wählen Sie **Advanced VPN Policies** (Erweiterte VPN-Richtlinien).
2. Klicken Sie im Bildschirm **VPN Policy** (VPN-Regel) auf die Option **Add Manual Policy** (Manuelle Regel hinzufügen).



Die folgenden Abschnitte beschreiben die Felder des Bildschirms **VPN - Manual Policy** (VPN - Manuelle Regel).

Allgemeine Einstellungen für die manuelle VPN-Regel

Im Folgenden werden die Felder mit den Netzwerkverbindungen für VPN-Tunnel aufgeführt:

- **Policy Name** (Name der Richtlinie): Geben Sie zur Kennzeichnung der Richtlinie einen eindeutigen Namen ein. Dieser Name wird nicht an den Remote-VPN-Endpunkt übermittelt. Er dient lediglich zur Verwaltung der Richtlinien.
- **Remote VPN Endpoint** (Remote-VPN-Endpunkt): Als Remote-VPN-Endpunkt muss die Adresse des aktuellen VPN-Gateways angegeben werden.

  Wenn der Remote-Endpunkt über eine dynamische IP-Adresse verfügt, wählen Sie **Dynamic IP Address** (Dynamische IP-Adresse). Es muss keine Adresse angegeben werden. Sie können mehrere dynamische Remote-IP-Regeln erstellen, es kann aber immer nur eine Regel aktiviert werden. Oder wählen Sie eine Option aus (**IP address** (IP-Adresse) oder **domain name** (Domainname)), und geben Sie die Adresse bzw. den Namen des Remote-VPN-Endpunkts ein, zu dem Sie eine Verbindung herstellen möchten

Lokale LAN-Einstellungen für die manuelle VPN-Regel

Bei diesen IP-Adressen handelt es sich um die Remote-Adressen für den Remote-VPN-Endpunkt.

- **Subnet Address** (Subnetzadresse): Geben Sie die Netzwerkmaske ein.
- **Single PC - no Subnet** (Einzelner PC - kein Subnetz): Wählen Sie diese Option, wenn sich am Remote-Endpunkt nur ein einzelner PC statt eines LAN befindet. Für diese Option sind keine weiteren Angaben erforderlich.
- **Single/Start IP Address** (Einzelne/Erste IP-Adresse): Die IP-Adresse für eine Einzeladresse oder die erste Adresse eines im LAN verwendeten Adressbereichs. Verwenden Sie eine Einzeladresse, wenn Sie Remote-Benutzern Zugriff auf einen einzelnen Server in Ihrem LAN gewähren möchten.
- **Any** (Beliebig): Für den Remote-VPN-Endpunkt können Sie eine beliebige IP-Adresse eingeben.
- **Finish IP Address** (Letzte IP-Adresse): Geben Sie die letzte IP-Adresse für den Adressbereich ein. Der Bereich muss dem Adressbereich Ihres LAN entsprechen.
- **Subnet Mask** (Subnetzmaske): Geben Sie die Netzwerkmaske ein.

Remote-LAN-Einstellungen für die manuelle VPN-Regel

Bei diesen IP-Adressen handelt es sich um die lokalen Adressen für den Remote-VPN-Endpunkt.

- **IP Address** (IP-Adresse): Wählen Sie die Option **Single PC - no Subnet** (Einzelne Adresse/Kein Subnetz), wenn sich am Remote-Endpunkt nur ein einzelner Computer statt eines LAN befindet. Für diese Option sind keine weiteren Angaben erforderlich. Typischerweise ist dies der Computer, auf dem sich der VPN-Client am Remote-Ende befindet.
- **Single/Start IP Address** (Einzelne/Erste IP-Adresse): Geben Sie am Remote-LAN eine IP-Adresse ein Mithilfe dieser Einstellungen können Sie auch auf einen Server zuzugreifen.
  - Geben Sie bei einem Adressbereich die erste IP-Adresse ein. Der Adressbereich muss im Remote-LAN vorhanden sein.
  - **Any** (Beliebig): Jeglicher von Computern in den Feldern Local IP (Lokale IP-Adresse) abgehende Datenverkehr löst einen VPN-Verbindungsversuch zum Remote-VPN-Endpunkt aus. Stellen Sie sicher, dass Sie diese Option wirklich anwenden möchten, bevor Sie sie auswählen.
- **Finish IP Address** (Letzte IP-Adresse): Geben Sie die letzte IP-Adresse für einen Adressbereich ein. Der Adressbereich muss im Remote-LAN vorhanden sein.
- **Subnet Mask** (Subnetzmaske): Geben Sie die Netzwerkmaske ein.

ESP-Einstellungen für die manuelle VPN-Regel

ESP (Encapsulating Security Payload) bietet Sicherheit für die Nutzinformationen (Daten), die durch den VPN-Tunnel gesendet werden.

- **SPI**: Geben Sie die erforderlichen SPIs (Security Policy Indexes) ein. Jede Regel benötigt eigene SPIs. Diese Einstellungen müssen mit dem Remote-VPN-Endpunkt übereinstimmen. Die Einstellung unter **in** (Eingang) muss mit der Einstellung unter **out** (Ausgang) am Remote-VPN-Endpunkt übereinstimmen, und die Einstellung unter **out** (Ausgang) muss der Einstellung unter **in** (Eingang) am Remote-VPN-Endpunkt entsprechen.
- **Encryption** (Verschlüsselung): Wählen Sie einen Verschlüsselungsalgorithmus, und geben Sie den Schlüssel in das Feld ein. 3DES-Schlüssel sollten aus 24 ASCII-Zeichen bestehen und DES-Schlüssel aus 8 ASCII-Zeichen.
  - **DES**: Der Data Encryption Standard (DES) verarbeitet eingehende Daten mit einer Breite von 64 Bit und verschlüsselt diese Werte mit einem 56-Bit-Schlüssel. Schneller, aber nicht so sicher wie 3DES.
  - **3DES**: (3DES) erreicht einen höheren Sicherheitsgrad, indem es die Daten dreimal mit DES und drei unterschiedlichen, voneinander unabhängigen Schlüsseln verschlüsselt.
- **Authentication** (Authentifizierung): Legen Sie die Authentifizierung und den Schlüssel fest.

Fehlerbehebung

8

Diagnostizieren und Lösen von Problemen

In diesem Kapitel finden Sie Informationen zur Behebung von Fehlern bei Ihrem N300 Wireless ADSL2+ Modemrouter (N300RMB). Nach der Beschreibung eines Problems finden Sie jeweils eine Anleitung zur Diagnose und Behebung des Problems.

Tipp: On Networks stellt hilfreiche Artikel, Dokumentationen und die aktuellen Softwareaktualisierungen unter *http://www.on-networks.com/support* bereit.

Dieses Kapitel enthält die folgenden Abschnitte:

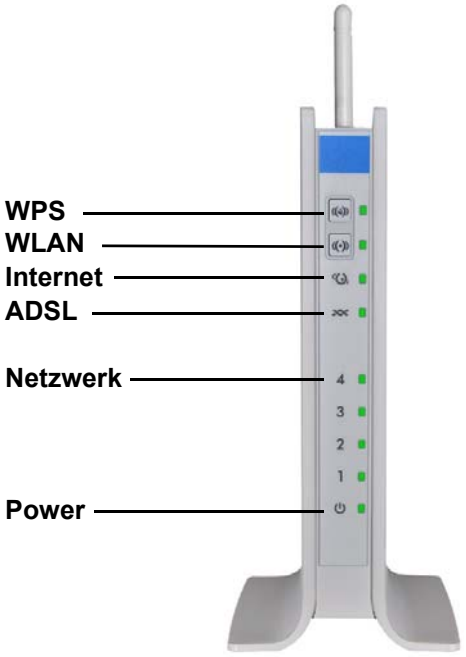
- *Beheben von Fehlern im Zusammenhang mit LEDs*
- *Anmeldung am Modemrouter nicht möglich*
- *Beheben von Fehlern bei der Internetverbindung*
- *TCP/IP-Netzwerk reagiert nicht*
- *Änderungen werden nicht gespeichert*
- *Falsches Datum oder falsche Uhrzeit*

Beheben von Fehlern im Zusammenhang mit LEDs

Wenn Sie das Gerät einschalten, sollten die Power-, LAN- und ADSL-LEDs wie hier beschrieben leuchten. Ist das nicht der Fall, suchen Sie in den folgenden Abschnitten nach Hilfe.

➢ **So überprüfen Sie die LEDs:**

1. Wenn das Gerät erstmals eingeschaltet wird, leuchtet die Power-LED.
2. Nach etwa 10 Sekunden leuchten die LAN- und die DSL-LED wie folgt:
   a. Die Netzwerk-Port-LEDs aller lokalen Ports, zu denen eine Verbindung besteht, leuchten.
   b. Die ADSL-LED leuchtet und zeigt somit an, dass eine Verbindung zum angeschlossenen Gerät besteht.



Power-LED leuchtet nicht

Wenn die Power-LED oder andere LEDs beim Einschalten des Modemrouters nicht aufleuchten, sollten Sie die folgenden Schritte durchführen:

- Vergewissern Sie sich, dass das Netzkabel ordnungsgemäß mit dem Modemrouter verbunden ist und dass das Netzteil ordnungsgemäß an eine funktionierende Steckdose angeschlossen ist.
- Prüfen Sie, ob Sie das Netzteil verwenden, das im Lieferumfang dieses Produkts enthalten war.

Falls sich der Fehler nicht beheben lässt, besteht ein Hardwareproblem. Wenden Sie sich an den technischen Support.

Power-LED leuchtet rot

Wenn der Modemrouter eingeschaltet wird, führt er einen Selbsttest durch, für dessen Dauer die Power-LED rot leuchtet. Falls die Power-LED nicht innerhalb etwa einer Minute grün wird, oder falls sie bei anderen Gelegenheiten während des normalen Betriebs rot wird, liegt ein Fehler im Modemrouter vor.

Wenn die Power-LED rot wird und damit einen Fehler im Modemrouter anzeigt, schalten Sie den Strom aus und wieder ein, um zu sehen, ob der Fehler im Modemrouter nur vorübergehend aufgetreten ist. Wenn die Power-LED eine Minute nach dem Einschalten immer noch rot leuchtet, gehen Sie wie folgt vor:

- Schalten Sie den Strom aus und wieder ein, um zu sehen, ob der Fehler im Modemrouter nur vorübergehend aufgetreten ist.
- Setzen Sie die Konfiguration des Modemrouters auf die werkseitigen Voreinstellungen zurück (siehe *Werkseinstellungen* auf Seite 113). Durch das Zurücksetzen der Konfiguration wird die IP-Adresse des Modemrouters auf 192.168.0.1 eingestellt.

Falls sich der Fehler nicht beheben lässt, besteht ein Hardwareproblem. Wenden Sie sich an den technischen Support.

Netzwerk-LED leuchtet nicht

Falls die entsprechende LAN-LED nicht leuchtet, wenn eine Netzwerkverbindung hergestellt wird, überprüfen Sie die folgenden Punkte:

- Das Netzwerkkabel muss fest in die Anschlüsse am Modemrouter und am Switch oder am Computer eingesteckt sein.
- Der angeschlossene Switch bzw. der Computer muss eingeschaltet sein.
- Sie verwenden das richtige Kabel.

Anmeldung am Modemrouter nicht möglich

Wenn Sie sich nicht über einen Computer im lokalen Netzwerk am Modemrouter anmelden können, überprüfen Sie die folgenden Punkte:

- Wenn Sie einen am Netzwerk angeschlossenen Computer verwenden, überprüfen Sie - wie im vorangehenden Abschnitt beschrieben - die Netzwerkverbindung zwischen dem Computer und dem Modemrouter.
- Vergewissern Sie sich, dass die IP-Adresse Ihres Computers zu demselben Subnetz gehört wie der Modemrouter. Wenn Sie das empfohlene Adressenschema verwenden, sollte die IP-Adresse des Computers im Bereich zwischen 192.168.0.2 bis 192.168.0.254 liegen.
- Wird als IP-Adresse des Computers 169.254.x.x angezeigt? Neuere Versionen von Windows und Mac OS erstellen eine IP-Adresse und weisen diese zu, wenn der Computer keinen DHCP-Server erreichen kann. Diese automatisch erstellten IP-Adressen liegen im Bereich 169.254.x.x. Wenn die IP-Adresse in diesem Bereich liegt, sollten Sie die Verbindung vom Computer zum Modemrouter überprüfen und den Computer neu starten.

- Wenn die IP-Adresse des Modemrouters sich geändert hat und Sie die aktuelle IP-Adresse nicht kennen, setzen Sie die Konfiguration des Modemrouters auf die werkseitigen Voreinstellungen zurück. Durch das Wiederherstellen der Werkseinstellungen wird die IP-Adresse desModemrouters auf 192.168.0.1 eingestellt. Eine Anleitung hierzu finden Sie unter *Werkseinstellungen* auf Seite 113.
- Vergewissern Sie sich, dass bei Ihrem Browser Java, JavaScript und ActiveX aktiviert sind. Wenn Sie den Internet Explorer verwenden, klicken Sie auf **Aktualisieren**, um sicherzugehen, dass das Java-Applet geladen wurde.
- Schließen Sie den Browser, und starten Sie ihn erneut.
- Vergewissern Sie sich, dass Sie die korrekten Anmeldedaten verwenden. Die werkseitigen Voreinstellungen sind wie folgt: Der Benutzername lautet **admin** und das Passwort **password**. Achten Sie darauf, dass beim Eingeben dieser Daten die Feststelltaste nicht aktiviert ist.

Beheben von Fehlern bei der Internetverbindung

Wenn der Modemrouter nicht auf das Internet zugreifen kann, überprüfen Sie zuerst die ADSL-Verbindung und dann die WAN-TCP/IP-Verbindung.

ADSL-Verbindung

Wenn der Modemrouter nicht auf das Internet zugreifen kann, überprüfen Sie zunächst, ob eine ADSL-Verbindung zum Provider besteht. Der Status dieser Verbindung wird durch die ADSL-LED angezeigt.

ADSL-LED leuchtet grün

Wenn die ADSL-LED grün leuchtet, haben Sie eine gute ADSL-Verbindung. Sie können davon ausgehen, dass der Provider die Verbindung ordnungsgemäß hergestellt hat und Sie alle Kabelverbindungen richtig eingesteckt haben.

ADSL-LED blinkt grün

Wenn die ADSL-LED grün blinkt, versucht der Modemrouter, eine ADSL-Verbindung zum Provider herzustellen. Die LED leuchtet innerhalb einiger Minuten grün auf.

Wenn dies nicht geschieht, trennen Sie alle Telefone von der Leitung. Wird das Problem dadurch behoben, schließen Sie die Telefone nacheinander wieder an (achten Sie dabei darauf, dass sich an jedem Telefon ein Mikrofilter befindet). Sind die Mikrofilter ordnungsgemäß angeschlossen, sollten Sie alle Telefone anschließen können.

Wenn das Problem durch das Entfernen der Telefone nicht behoben werden konnte, sind die Leitungen möglicherweise fehlerhaft. Hat die Telefongesellschaft das DSL-Signal an Ihrem Netzabschlussgerät (Network Interface Device, NID) überprüft, sind die Leitungen in Ihrem Haus möglicherweise von ungenügender Qualität.

ADSL-LED leuchtet nicht

Wenn die ADSL-LED nicht leuchtet, trennen Sie alle Telefone von der Leitung. Wird das Problem dadurch behoben, schließen Sie die Telefone nacheinander wieder an (achten Sie dabei darauf, dass sich an jedem Telefon ein Mikrofilter befindet). Sind die Mikrofilter ordnungsgemäß angeschlossen, sollten Sie alle Telefone anschließen können.

Leuchtet die ADSL-LED nach dem Trennen der Telefone immer noch nicht grün, überprüfen Sie die folgenden Punkte:

- Stellen Sie sicher, dass die Telefongesellschaft die Verbindung zu Ihrer Leitung freigeschaltet und getestet hat.
- Überprüfen Sie, ob Sie mit der richtigen Telefonleitung verbunden sind. Wenn Sie über mehr als eine Telefonleitung verfügen, stellen Sie sicher, dass Sie mit der ADSL-Leitung verbunden sind. Möglicherweise müssen Sie einen Adapter verwenden, wenn sich das ADSL-Signal auf Pins 1 und 4 des RJ-11-Steckers befindet. Für den Modemrouter werden die Pins 2 und 3 verwendet.

Internet-LED leuchtet rot

Die Internet-LED leuchtet rot, wenn das Gerät keine Verbindung zum Internet herstellen konnte. Überprüfen Sie Folgendes:

- Überprüfen Sie Ihre Anmeldedaten oder die Daten, die Sie im Bildschirm **Basic Settings** (Grundeinstellungen) eingegeben haben.
- Wenden Sie sich an Ihren ISP, um zu überprüfen, ob die Einstellungen für das Multiplexverfahren, VPI und VCI auf dem Bildschirm **ADSL Settings** (ADSL-Einstellungen) korrekt sind.
- Überprüfen Sie, ob ein Problem bei Ihrem ISP vorliegt - möglicherweise liegt es nicht daran, dass der Modemrouter keine Verbindung zum Internet herstellen kann, sondern daran, dass Ihr ISP keine Internetverbindung zur Verfügung stellen kann.

Abrufen einer Internet IP-Adresse

Wenn Ihr Modemrouter keinen Zugriff auf das Internet hat und die Internet-LED grün leuchtet, überprüfen Sie, ob der Modemrouter eine Internet IP-Adresse vom ISP abrufen kann. Wurde Ihnen keine statische IP-Adresse zugewiesen, fordert der Modemrouter eine IP-Adresse vom ISP an. Mithilfe der Browseroberfläche können Sie überprüfen, ob die Anforderung erfolgreich war.

➢ **So überprüfen Sie die Internet IP-Adresse über die Browseroberfläche:**

1. Starten Sie den Browser, und wählen Sie eine externe Website.
2. Rufen Sie das Hauptmenü der Modemrouter-Konfiguration unter http://192.168.0.1 auf.
3. Überprüfen Sie im Startbildschirm (Routerstatus), ob für den WAN-Port eine IP-Adresse angezeigt wird. Wenn 0.0.0.0 angezeigt wird, konnte der Modemrouter keine IP-Adresse vom Internet-Provider abrufen.

Wenn der Modemrouter keine IP-Adresse vom ISP beziehen kann, kann dies folgende Ursachen haben:

- Wenn Sie ein Anmeldeprogramm ausgewählt haben, könnte der Dienstname, der Benutzername oder das Password falsch eingerichtet worden sein. Siehe hierzu den folgenden Abschnitt *Beheben von Fehlern im Zusammenhang mit PPPoE oder PPPoA*.
- Der ISP überprüft vielleicht den Hostnamen des Computers. Weisen Sie im Browser-basierten Setup-Assistenten dem Modemrouter den Hostnamen des Internetkontos zu.
- Der ISP erlaubt nur einer MAC-Adresse den Verbindungsaufbau zum Internet und überprüft die MAC-Adresse Ihres Computers. Wählen Sie in diesem Fall eine der folgenden Optionen:
  - Teilen Sie dem ISP mit, dass Sie ein neues Netzwerkgerät erworben haben, und bitten Sie darum, die MAC-Adresse des Modemrouters zu verwenden.
  - Konfigurieren Sie Ihren Modemrouter so, dass er seine MAC-Adresse fälscht, indem er die des Computers verwendet. Dies können Sie im Bildschirm **Basic Settings** (Grundeinstellungen) durchführen.

Beheben von Fehlern im Zusammenhang mit PPPoE oder PPPoA

➢ **So beheben Sie Probleme mit der PPPoE- oder PPPoA-Verbindung:**

1. Melden Sie sich unter dieser Adresse am Modemrouter an: http://192.168.0.1.
2. Klicken Sie im Startbildschirm auf die Schaltfläche **Connection Status** (Verbindungsstatus).
3. Wenn alle Felder sinnvolle Werte wie **OK** anzeigen, funktioniert die PPPoE- bzw. PPPoA-Verbindung fehlerfrei.
4. Wird bei einem der Schritte ein Fehler oder ein leeres Feld angezeigt, können Sie durch Klicken auf **Connect** (Verbinden) erneut versuchen, eine Verbindung herzustellen. Der Modemrouter versucht immer wieder, eine Verbindung herzustellen.

Wenn Sie nach einigen Minuten immer noch keine Verbindung herstellen können, ist ggf. der verwendete Dienstname, der Benutzername oder das angegebene Kennwort falsch. Möglicherweise liegt auch bei Ihrem ISP ein Problem vor.

Hinweis: Wenn Sie die Verbindung nicht manuell herstellen, findet eine Authentifizierung seitens des Modemrouters über PPPoE bzw. PPPoA erst dann statt, wenn Daten an das Netzwerk übertragen werden.

Fehlerbehebung im Zusammenhang mit dem Internetzugriff

Wenn der Modemrouter eine IP-Adresse erhält, Sie aber dennoch keine Webseiten aus dem Internet anzeigen können, kann dies folgende Ursachen haben:

- Ihr Computer erkennt möglicherweise keine DNS-Serveradressen.

  Ein DNS-Server ist ein Host im Internet, der Internetnamen (z. B. www-Adressen) in numerische IP-Adressen umwandelt. Normalerweise stellt der Internet-Provider Ihnen die Adressen von einem oder zwei DNS-Servern automatisch zur Verfügung. Wenn Sie bei der Einrichtung des Modemrouters eine DNS-Adresse eingegeben haben, starten Sie den Computer neu, und überprüfen Sie die DNS-Adresse. Sie können die DNS-Adressen aber auch manuell auf dem Computer konfigurieren. Hinweise dazu finden Sie in der Dokumentation zu Ihrem Betriebssystem.

- Der Modemrouter ist auf dem Computer nicht als TCP/IP-Modemrouter konfiguriert.

  Wenn der Computer seine Daten über DHCP vom Modemrouter bezieht, starten Sie den Computer neu, und überprüfen Sie die Modemrouter-Adresse.

TCP/IP-Netzwerk reagiert nicht

Die meisten TCP/IP-Terminals und Router verfügen über ein Ping-Dienstprogramm, das ein Echo-Request-Paket an das angegebene Gerät sendet. Das Gerät reagiert mit einem Echo, um mitzuteilen, ob ein TCP/IP-Netzwerk auf Anfragen reagiert.

Testen des LAN-Pfads zum Modemrouter

Sie können vom Computer aus ein Ping-Signal an den Modemrouter senden, um zu überprüfen, ob der LAN-Pfad zum Modemrouter richtig eingerichtet ist.

➢ **So senden Sie von einem Computer mit Windows 95 oder höher ein Ping-Signal an den Modemrouter:**

1. Klicken Sie in der Windows Taskleiste auf die Schaltfläche **Start**, und wählen Sie **Ausführen**.
2. **Geben Sie im Eingabefeld ping** gefolgt von der IP-Adresse des Modemrouters ein. Beispiel:

   ping 192.168.0.1

3. Klicken Sie auf **OK**.

   Daraufhin wird eine Meldung wie die folgende angezeigt:

   ```
   Ping wird ausgeführt für <IP address> mit 32 Bytes Daten
   ```

   Wenn der Pfad funktioniert, wird diese Nachricht angezeigt:

   ```
   Antwort von <IP address>: Bytes=32 Zeit=NNms TTL=xxx
   ```

Wenn der Pfad nicht funktioniert, wird diese Nachricht angezeigt:

```
Zeitüberschreitung der Anforderung
```

Wenn der Pfad nicht richtig funktioniert, könnte eines der folgenden Probleme vorliegen:

- Fehlerhafte physikalische Verbindung
  - Vergewissern Sie sich, dass die LED des Netzwerkports leuchtet. Falls die LED nicht leuchtet, befolgen Sie die Anweisungen unter *Netzwerk-LED leuchtet nicht* auf Seite 105.
  - Vergewissern Sie sich, dass die Verbindungs-LEDs für die Netzwerkkarten- und Switch-Ports (falls vorhanden), die mit der Workstation und dem Modemrouter verbunden sind, leuchten.
- Fehlerhafte Netzwerkkonfiguration
  - Vergewissern Sie sich, dass die Treiber für die Netzwerkkarte sowie die TCP/IP-Software auf dem Computer bzw. der Workstation installiert und richtig konfiguriert sind.
  - Vergewissern Sie sich, dass die IP-Adressen des Modemrouters und des Computers korrekt sind und dass die Adressen zum selben Subnetz gehören.

Testen des Pfads vom Computer zu einem Remote-Gerät

Nachdem Sie sich vergewissert haben, dass die LAN-Pfade einwandfrei funktionieren, sollten Sie den Pfad vom Computer zu einem Remote-Gerät testen. Geben Sie unter Windows im Fenster **Ausführen** die folgende Anweisung ein:

```
ping -n 10 IP-Adresse
```

Setzen Sie dabei anstelle von „IP-Adresse“ die IP-Adresse eines Remote-Geräts (z. B. des DNS-Servers des ISP) ein.

Wenn der Pfad einwandfrei funktioniert, werden dieselben Antworten wie in *Testen des LAN-Pfads zum Modemrouter* auf Seite 109 angezeigt. Falls Sie keine Antworten erhalten, überprüfen Sie Folgendes:

- Ihr Computer muss eine IP-Adresse aus demselben Subnetz wie der Modemrouter haben, der als Standard-Modemrouter eingerichtet ist. Wenn die IP-Konfiguration Ihres Computers über DHCP erfolgt ist, werden diese Informationen nicht unter der Option **Network** (Netzwerk) in der Systemsteuerung angezeigt. Vergewissern Sie sich, dass die IP-Adresse des Modemrouters als Standardrouter eingerichtet ist.
- Die Netzwerkadresse des Computers (der Abschnitt der IP-Adresse, der durch die Netzmaske festgelegt wird) muss sich von der Netzwerkadresse des Remote-Geräts unterscheiden.
- Das Kabel- oder DSL-Modem muss angeschlossen und in Betrieb sein.
- Wenn der ISP dem Computer einen Hostnamen zugewiesen hat, geben Sie unter **Basic Settings** (Grundeinstellungen) diesen Hostnamen als Kontonamen ein.

- Vielleicht akzeptiert der Internet-Provider nur die MAC-Adresse eines einzigen Ihrer Computer und lehnt alle anderen ab. Viele Breitbandanbieter schränken den Zugang ein, indem sie nur Datenverkehr von der MAC-Adresse Ihres Modems zulassen. Manche Internet-Provider schränken den Zugang jedoch noch zusätzlich auf die MAC-Adresse eines einzelnen, an dieses Modem angeschlossenen Computers ein. Konfigurieren Sie in diesem Fall Ihren Modemrouter so, dass er die MAC-Adresse des berechtigten Computers dupliziert oder „fälscht“.

Änderungen werden nicht gespeichert

Wenn der Modemrouter die über die Modemrouter-Benutzeroberfläche vorgenommenen Änderungen nicht speichert, überprüfen Sie die folgenden Punkte:

- Nach der Eingabe der Konfigurationseinstellungen müssen Sie immer auf die Schaltfläche **Apply** (Übernehmen) klicken, bevor Sie zu einem anderen Bildschirm oder einer anderen Registerkarte wechseln. Anderenfalls gehen Ihre Änderungen verloren.
- Klicken Sie im Webbrowser auf die Schaltfläche **Refresh** (Aktualisieren) bzw. **Reload** (Erneut laden). Es kann sein, dass die Änderungen zwar vorgenommen wurden, im Cache des Webbrowsers jedoch noch die alte Konfiguration gespeichert ist.

Falsches Datum oder falsche Uhrzeit

Wählen Sie **Security** (Sicherheit) > **Schedule** (Zeitplan) aus, um das aktuelle Datum und die aktuelle Uhrzeit anzuzeigen. Der Modemrouter nutzt das NTP (Network Time Protocol) zum Abruf der aktuellen Uhrzeit von einem der NTP-Server im Internet. Jeder Protokolleintrag wird mit Datum und Uhrzeit versehen. Im Zusammenhang mit Datum und Uhrzeit können u. a. die folgenden Probleme auftreten:

- Als Datum wird der 1. Januar 2000 angezeigt. Der Modemrouter konnte noch keine Verbindung zu einem NTP-Server herstellen. Vergewissern Sie sich, dass der Internetzugang richtig konfiguriert ist. Wenn Sie die Konfiguration des Modemrouters abgeschlossen haben, warten Sie mindestens fünf Minuten, und überprüfen Sie dann das Datum und die Uhrzeit erneut.
- Die Zeit weicht um eine Stunde ab. Dieses Modem verfügt über eine automatische Umstellung zwischen Sommer- und Winterzeit. Um diese Funktion zu nutzen, stellen Sie sicher, dass im Bildschirm **Schedule** (Zeitplan) das Kontrollkästchen **Automatically adjust for daylight savings time** (Automatisch an Sommer-/Winterzeit anpassen) aktiviert ist.

Zusatzinformationen

A

In diesem Anhang werden die folgenden Themen behandelt:

- *Werkseinstellungen*
- *Technische Daten*

Werkseinstellungen

Sie können den Modemrouter auf die Werkseinstellungen zurücksetzen. Drücken Sie die **Reset**-Taste auf der Rückseite des mit einer Büroklammer oder einem ähnlichen Gegenstand ein, und halten Sie sie mindestens 7 Sekunden lang gedrückt.

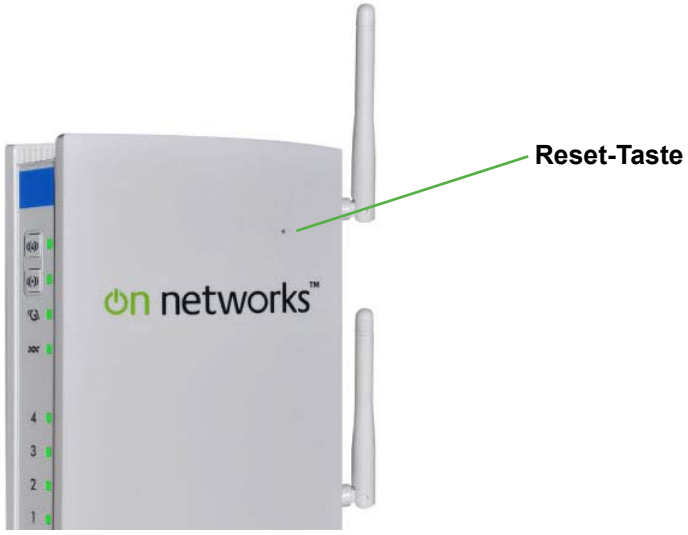


Abbildung 10. Reset-Taste

Der Modemrouter wird auf die in der folgenden Tabelle angegebenen Werkseinstellungen zurückgesetzt:

Tabelle 4. Werkseitige Voreinstellungen

Funktion		Standardeinstellungen
Router-Anmeldung	Adresse zur Benutzeranmeldung	http://www.mywifirouter.com
	Benutzername (Groß- und Kleinschreibung beachten)	admin
	Anmeldepasswort (Groß- und Kleinschreibung beachten)	admin
Internetverbindung	WAN-MAC-Adresse	Standardadresse verwenden
	WAN-MTU-Größe	1492
	Portgeschwindigkeit	Automatische Erkennung

Tabelle 4. Werkseitige Voreinstellungen (Fortsetzung)

Funktion		Standardeinstellungen
Lokales Netzwerk (LAN)	LAN-IP	192.168.0.1
	Subnetzmaske	255.255.255.0
	RIP-Richtung	Keine
	RIP-Version	Deaktiviert
	RIP-Authentifizierung	Keine
	DHCP-Server	Aktiviert
Lokales Netzwerk (LAN) (Fortsetzung)	Erste IP-Adresse für DHCP	192.168.0.2
	Letzte IP-Adresse für DHCP	192.168.0.254
	DMZ	Aktiviert oder deaktiviert
	Zeitzone	GMT für WW außer NA und GR, GMT+1 für GR, GMT-8 für NA
	Berücksichtigung der Sommerzeit	Deaktiviert
	SNMP	Deaktiviert
Firewall	Eingehend (Daten, die aus dem Internet eingehen)	Gesperrt (mit Ausnahme des Verkehrs über den HTTP-Port 80)
	Ausgehend (Daten, die ins Internet gesendet werden)	Aktiviert (alle ausgehenden Daten können passieren)
	MAC-Filterung	Deaktiviert

Tabelle 4. Werkseitige Voreinstellungen (Fortsetzung)

Funktion		Standardeinstellungen
WLAN	Drahtlose Kommunikation	Aktiviert
	Netzwerkname (SSID)	*OnNetworksXX* (wobei XX für zwei beliebige Zeichen steht) Befindet sich auf dem Etikett an der Unterseite des Geräts.
	WLAN-Passwort	*XXXXXXXX* (8 beliebige Zeichen)
	Sicherheit	Gemischt: WPA2-PSK
	Netzwerknamen (SSID) übertragen	Aktiviert
	Land/Region	Europa
	RF-Kanal	Auto
	Operationsmodus	Bis zu 300 MBit/s:
	Übertragungsrate	Bestmöglich
	Ausgangsleistung	Vollduplex
	Access Point	Aktiviert
	Authentifizierungsverfahren	Pre-Shared Key
	Liste der zugriffsberechtigten WLAN-Karten	Alle WLAN-Geräte zugelassen

Technische Daten

Tabelle 5. Technische Daten

Funktion	Beschreibung
Daten- und Routingprotokolle	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE oder PPPoA, RFC 1483 Bridged oder Routed Ethernet und RFC 1577 Classical IP over ATM
Netzstecker an Land angepasst	110 V-220 V, 50/60 Hz, Eingangsspannung
Abmessungen	200 x 113,4 x 86,2 mm
Gewicht	0,285 kg
Betriebstemperatur	0° bis 40°C
Luftfeuchtigkeit	90 % maximale relative Luftfeuchtigkeit, nicht kondensierend

Tabelle 5. Technische Daten (Fortsetzung)

Funktion	Beschreibung
Einhaltung der Richtlinien	EN 55022/24 (CISPR 22/24) Klasse B EN 60950 (CE LVD) Klasse B EN 301 489-17 V.2.1.1 (2009) EN 301 489-1 V1.9.2 (2011) EN 300 328 V1.7.1 (2006) K21:ITU-T K.21- 07/2003 TBR21: TBR21 Januar 1998
Technische Daten zu den Schnittstellen	LAN: 10BASE-T oder 100BASE-TX, RJ-45 WAN: ADSL, Dual-RJ-11, Pins 2 und 3 ANSI T1.413, ITU G.992.1 (G.DMT), ITU G.992.2 (G.Lite) ITU Anhang A Hardware oder Anhang B Hardware ITU G.992,5 (ADSL2+)

Konformitätserklärung

B

WLAN-Router, Gateways, APs

Informationen zur Einhaltung rechtlicher Vorschriften

Hinweis: Dieser Abschnitt enthält die an den Benutzer gestellten Anforderungen für den Betrieb dieses Produkts gemäß der nationalen Gesetze für die Nutzung von Frequenzen und den Betrieb von Funkanlagen. Sollte der Endbenutzer die einschlägigen rechtlichen Vorgaben nicht einhalten, kann dies zu einem rechtswidrigen Betrieb führen, der wiederum dazu führen kann, dass die entsprechende nationale Behörde ein Verfahren gegen den Endbenutzer einleitet.

Hinweis: Die Firmware dieses Produkts beschränkt den Betrieb des Geräts auf die Kanäle, die in den jeweiligen Ländern oder Regionen zulässig sind. Aus diesem Grund stehen möglicherweise nicht alle in diesem Benutzerhandbuch beschriebenen Optionen für Ihre Version des Produkts zur Verfügung.

Europa - EU-Konformitätserklärung

CE !

Die Kennzeichnung mit dem o. a. Symbol gibt an, dass die verbindlichen Anforderungen der R&TTE-Richtlinie der Europäischen Union (1999/5/EC) erfüllt werden. Dieses Gerät erfüllt die folgenden Normen:

EN300 328 (2,4 Ghz), EN301 489-17 EN60950-1

Die vollständige EU-Konformitätserklärung finden Sie unter: *http://www.on-networks.de/doc.*

EU-Konformitätserklärung in den Sprachen der Europäischen Gemeinschaft

Sprache	Erklärung
Cesky [Tschechisch]	*On Networks* tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Dänisch]	Undertegnede *On Networks* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch	Hiermit erklärt *On Networks*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estnisch]	Käesolevaga kinnitab *On Networks* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

English [Englisch]	Hereby, *On Networks* declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanisch]	Por medio de la presente *On Networks* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Griechisch]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *On Networks* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [Französisch]	Par la présente *On Networks* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italienisch]	Con la presente *On Networks* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Lettisch]	Ar šo *On Networks* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Litauisch]	Šiuo *On Networks* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Niederländisch]	Hierbij verklaart *On Networks* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltesisch]	Hawnhekk, *On Networks* jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Ungarisch]	Alulírott, *On Networks* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polnisch]	Niniejszym On Networks oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portugiesisch]	*On Networks* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slowenisch]	On Networks izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slowakisch]	*On Networks* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnisch]	*On Networks* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska [Schwedisch]	Härmed intygar *On Networks* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Isländisch]	Hér með lýsir *On Networks* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegisch]	*On Networks* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Das Gerät ist ein 2,4-GHz-Breitband-Übertragungsgerät (Transceiver), das in allen Mitgliedsstaaten der EU und der EFTA eingesetzt werden darf, mit Ausnahme von Frankreich und Italien, wo nur eine eingeschränkte Nutzung möglich ist.

In Italien sollte der Endbenutzer eine Lizenz bei der nationalen Behörde für Funkfrequenzen beantragen, um eine Genehmigung für die Einrichtung von Funkverbindungen in Außenbereichen und/oder die Bereitstellung von öffentlichem Zugang zu Telekommunikations- oder Netzwerkdiensten zu erhalten.

Dieses Gerät darf in Frankreich nicht für die Einrichtung von Funkverbindungen in Außenbereichen eingesetzt werden, und in manchen Gebieten kann die zulässige äquivalente isotrope Sendeleistung (EIRP) der Funkfrequenzen im Bereich zwischen 2454 und 2483,5 MHz auf 10 mW begrenzt sein. Detaillierte Informationen hierzu sollte der Endbenutzer bei der nationalen Behörde für Funkfrequenzen in Frankreich einholen.

Richtlinien der FCC für den Betrieb in den USA

FCC-Informationen für den Benutzer

Dieses Produkt enthält keine Komponenten, die vom Benutzer gewartet werden können, und darf nur mit dafür zugelassenen Antennen eingesetzt werden. Jegliche Änderungen oder Modifikationen am Produkt führen zum Erlöschen sämtlicher gesetzlicher Zertifizierungen und Zulassungen.

FCC-Richtlinien zur Strahlungsexposition

Die Strahlung dieses Geräts liegt unter den von der FCC festgelegten Grenzwerten für Hochfrequenzstrahlung in einer unkontrollierten Umgebung. Bei der Installation und Verwendung dieses Geräts sollte ein Abstand von mindestens 20 cm zwischen der Strahlungsquelle und Ihrem Körper eingehalten werden.

Dieser Sender darf nicht in der Nähe von oder in Verbindung mit anderen Antennen oder Sendern betrieben werden.

FCC-Konformitätserklärung

Wir, On Networks, 350 East Plumeria Drive, Santa Jose, CA 95134, erklären unter alleiniger Verantwortung, dass der N300 Wireless ADSL2+ Modemrouter (N300RMB) mit Teil 15, Unterabschnitt B der FCC-Vorschriften CFR47 konform ist. Der Betrieb unterliegt den folgenden Bedingungen:

- Dieses Gerät darf keine gesundheitsschädlichen Störungen verursachen und
- Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Operationen verursachen können.

FCC-Warnungen und -Hinweise zu Hochfrequenzstörungen

Dieses Gerät wurde geprüft, und es wurde festgestellt, dass es die Grenzwerte für Digitalgeräte der Klasse B gemäß Teil 15 der FCC-Vorschriften einhält. Diese Grenzwerte sind für die Gewährleistung eines angemessenen Schutzes gegen schädliche Störungen bei der Installation im Wohnbereich gedacht. Dieses Gerät verwendet Funkwellen und kann diese abstrahlen. Wenn es nicht gemäß den Anleitungen installiert und verwendet wird, kann es zu erheblichen Störungen von Funkübertragungen kommen. Bei keiner Installation können Störungen jedoch völlig ausgeschlossen werden. Wenn dieses Gerät Störungen des Rundfunk- und Fernsehempfangs verursacht, was durch Ein- und Ausschalten des Gerätes festgestellt werden kann, sollte der Benutzer versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Platzieren Sie die Empfangsantenne an einer anderen Stelle bzw. richten Sie sie neu aus.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.

- Schließen Sie das Gerät an einen Stromkreis an, den der Empfänger nicht benutzt.
- Wenden Sie sich an den Händler oder einen erfahrenen Rundfunk-/TV-Techniker.

FCC-Warnung

- Veränderungen oder Modifikationen, die nicht ausdrücklich durch die für die Konformität zuständige Stelle genehmigt sind, könnten die Berechtigung des Benutzers zum Betreiben des Gerätes ungültig machen.
- Dieses Gerät ist mit Teil 15 der FCC-Vorschriften konform. Der Betrieb unterliegt den folgenden Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen. (2) Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Funktionen verursachen können.
- Produkte für den Markt in den USA können nur auf den Kanälen 1 - 11 betrieben werden. Die Auswahl anderer Kanäle ist nicht möglich.
- Dieses Gerät und die zugehörige(n) Antenne(n) dürfen nicht in der Nähe von oder in Verbindung mit anderen Antennen oder Sendern betrieben werden.

Kanadisches Ministerium für Kommunikation (Department of Communications) – Vorschriften zu Funkstörungen

Dieses digitale Gerät (N300 Wireless ADSL2+ Modemrouter (N300RMB)) überschreitet nicht die Grenzwerte der Klasse B für von digitalen Geräten ausgehende Funkstörungen, wie sie in den Vorschriften zu Funkstörungen des kanadischen Ministeriums für Kommunikation festgelegt sind.

Dieses Digitalgerät der Klasse [B] entspricht dem kanadischen Standard ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

Dieses Gerät stimmt mit RSS-210 der Regeln von Industry Canada überein. Der Betrieb unterliegt den folgenden Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen. (2) Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Funktionen verursachen können.

WICHTIGER HINWEIS: Erklärung zur Strahlenbelastung:

Die Strahlung dieses Geräts liegt unter den von IC festgelegten Grenzwerten für Hochfrequenzstrahlung in einer unkontrollierten Umgebung. Bei der Installation und Verwendung dieses Geräts sollte ein Abstand von mindestens 20 cm zwischen der Strahlungsquelle und Ihrem Körper eingehalten werden.

Achtung:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Tabelle für die Reduzierung von Funkstörungen

In der nachfolgenden Tabelle wird der empfohlene Mindestabstand zwischen On Networks-Geräten und -Haushaltsgeräten zur Reduzierung von Funkstörungen angegeben (in Metern und Fuß).

Haushaltsgerät	Empfohlener Mindestabstand (in Metern und Fuß)
Mikrowellengeräte	9 Meter (30 Fuß)
Babyfon – analog	6 Meter (20 Fuß)
Babyfon – digital	12 Meter (40 Fuß)
Schnurloses Telefon – analog	6 Meter (20 Fuß)
Schnurloses Telefon – digital	9 Meter (30 Fuß)
Bluetooth-Geräte	6 Meter (20 Fuß)
ZigBee	6 Meter (20 Fuß)